HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

DIPLOMARBEIT

Ing. Romed Giner

Informationssicherheits-konzept für die Integration von medizintechnischen Geräten in ein IT-Datennetz

Mittweida, 2011

Fakultät Elektro- und Informationstechnik

DIPLOMARBEIT

Informationssicherheits-konzept für die Integration von medizintechnischen Geräten in ein IT-Datennetz

Autor:
Ing. Romed Giner

Studiengang:
Informationstechnik

Seminargruppe:
KI09wIA

Erstprüfer:
Prof. habil. Ing. Dr. Lutz Winkler

Zweitprüfer:
Ing. Mag. Dr. Marko Überegger

Einreichung:
Mittweida, Juli 2011

Bibliografische Angaben:
Giner, Romed

Informationssicherheitskonzept für die Integration von medizintechnischen Geräten in ein IT-Datennetz

Mittweida, Hochschule Mittweida (FH), University of Applied Sciences, Fakultät Elektro- und Informationstechnik, Diplomarbeit, 2011

Referat:

Medizintechnik und Informationstechnik wachsen durch die Integration verschiedenster medizintechnischer Systeme in das IT-Datennetz immer mehr zusammen und bilden dadurch ein sogenanntes medizinisches Netzwerk.
An dieses medizinische Netzwerk werden besondere Anforderungen gestellt, um den speziellen Bedürfnissen der medizintechnischen Geräte im laufenden Betrieb gerecht zu werden.
Diese Geräte müssen im Hinblick auf die Verarbeitung, Speicherung und Übertragung von Informationen, bezüglich Vertraulichkeit, Verfügbarkeit und Integrität vor negativen Beeinflussungen durch organisatorische und technische Maßnahmen geschützt werden.
Zielsetzung dieser Diplomarbeit ist die Entwicklung eines Informationssicherheitskonzeptes zur Gewährleistung der Betriebssicherheit der eingebundenen medizintechnischen Geräte in das IT-Datennetz.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AES	Advanced-Encryption-Standard
AGW	Application-Gateways
ASCII	American Standard Code for Information Interchange
BSI	Bundesamt für Sicherheit in der Informationstechnik
CE	CE-Kennzeichnung
CSRF	Cross-Site Request-Forgery
CVP	Content Vectoring Protocol
DDoS	Distributed-Denial-of-Service
DES	Data-Encryption-Standard
DIN	Deutsches Institut für Normung
DMZ	Demilitarized Zone
DNS	Domain-Name-System
DoS	Denial of Service
DPI	Deep-Packet-Inspection
EDV	Elektronische Datenverarbeitung
EEG	Elektroenzephalografie
EKG	Elektrokardiogramm
EWG	Europäische Wirtschaftsgemeinschaft
FTP	File-Transfer-Protocol
GMP	Good-Manufacturing-Practice
HIPS	Host-based Intrusion-Prevention-System
HTTP	Hypertext-Transfer-Protocol
ICMP	Internet-Control-Message-Protocol
IDS	Intrusion-Detection-System
IEC	Internationale Elektrotechnische Kommission
IEEE	Institute of Electrical and Electronics Engineers
IMAP	Internet-Message-Access-Protocol
IPS	Intrusion-Prevention-System
IPsec	Internet-Protocol-Security
ISO	International Organization for Standardization
IT	Informationstechnologie
KIS	Klinisches Informationssystem

LAN	Local Area network
LDAP	Lightweight-Directory-Access-Protocol
LIS	Labor-Informations-System
MAC	Media-Access-Control
MP	Medizinprodukt
MPBV	Medizinprodukte-Betreiberverordnung
MPG	Medizinproduktegesetz
MTK	Messtechnische Kontrollen
NAT	Network-address-translation
NIPS	Network-based Intrusion-Prevention-System
NMS	Network Management Software
OP	Operation-System
OSI	Open Systems Interconnection Model
PDF	Portable-Document-Format
PHP	Hypertext-Preprocessor
POP	Post-Office-Protocol
QoS	Quality of Service
RPC	Remote-Procedure-Call
SMTP	Simple-Mail-Transfer-Protocol
SOI	Service Oriented Infrastructure
SPI	Stateful-Packet-Inspection
SQL	Structured-Query-Language
SSH	Secure Shell
STK	Sicherheitstechnische Prüfung
TCP	Transmission-Control-Protocol
TILAK	Tiroler Landeskrankenanstalten GmbH
TSB	Technische/r Sicherheitsbeauftragte
UDP	User-Datagram-Protocol
URL	Uniform-Resource-Locator
VLAN	Virtual Local Area-Network
WAN	Wide Area-Network
WLAN	Wireless Local Area-Network
XSS	Cross-Site-Scripting

1 Einleitung und Übersicht

Medizintechnik und Informationstechnik wachsen durch die Integration verschiedenster medizintechnischer Systeme in das IT-Datennetz immer mehr zusammen und bilden dadurch ein sogenanntes medizinisches Netzwerk.
An dieses medizinische Netzwerk werden besondere Anforderungen gestellt, um den speziellen Bedürfnissen der Medizinprodukte im laufenden Betrieb gerecht zu werden.
Eine besondere Herausforderung stellen sogenannten „Aktive Medizinprodukte“ z.B. Beatmungsgeräte, Herz-Lungen-Maschinen usw. an den Betreiber dar und sind daher als besonders kritisch in der Betriebsführung einzustufen.
Daher muss der Bereich Informationstechnik in besonderem Maße mit der Medizintechnik kooperieren, um diese neuen Herausforderungen in Bezug auf Verfügbarkeit, Integrität, Verfügbarkeit, Authentizität, Verlässlichkeit und Datenschutz bewältigen zu können. Weiters müssen gemeinsame Betriebskonzepte und Verantwortungsbereiche definiert werden, um auch den gesetzlichen Anforderungen gerecht zu werden.

1.1 Ausgangssituation

Derzeit sind medizintechnische Geräte häufig ohne besondere Schutzmechanismen in das interne IT-Datennetz (Intranet) eingebunden. Die Systeme verfügen nur zum Teil über einen ausreichenden Schutz z.B. vor möglicher Schadsoftware und entsprechen nicht den IT-Sicherheitsrichtlinien der eingebundenen IT-Arbeitsplätze.
Die Geräte sind teilweise als Gesamtsystem zertifiziert und es dürfen keine Änderungen an den Systemen vorgenommen werden. Zusätzliche IT-Schutzsoftware bzw. die Einspielung von Sicherheitsupdates ist durch Richtlinien der Hersteller untersagt.

1.2 Motivation

Die zur PatientInnen-Behandlung notwendigen medizintechnischen Geräte sollen im Hinblick auf die Verarbeitung, Speicherung und Übertragung von Informationen bezüglich Vertraulichkeit, Verfügbarkeit und Integrität vor negativen Beeinflussungen geschützt werden.

1.3 **Fragestellung**

Können medizintechnische Geräte im Hinblick auf die Verarbeitung, Speicherung und Übertragung von Informationen, bezüglich Vertraulichkeit, Verfügbarkeit und Integrität vor negativen Beeinflussungen durch spezielle organisatorische und technische Maßnahmen geschützt werden?

1.4 **Zielsetzung**

Entwicklung eines Informationssicherheitskonzeptes zur Gewährleistung der Betriebssicherheit der eingebundenen medizintechnischen Geräte in das IT-Datennetz und Schutz dieser Geräte vor möglichen Bedrohungen und den daraus entstehenden Betriebsausfällen.

1.5 **Kapitelübersicht**

Im **Kapitel 1** werden die allgemeinen Ziele wie Ausgangssituation, Motivation, Fragestellung und Zielsetzung bei der Integration von medizintechnischen Geräten in ein IT-Datennetz behandelt.

Die Grundlagen der Sicherheitsziele im IT-Netzwerk, im OSI-Modell und die möglichen technischen und organisatorischen Gefährdungen sowie die rechtlichen Grundlagen werden im **Kapitel 2** behandelt.

Die möglichen technischen Maßnahmen, um potenziellen Gefährdungen, welche im Kapitel 2 behandelt werden, entgegenwirken zu können, werden im **Kapitel 3** beschrieben.

Die IST-Analyse der eingesetzten medizintechnischen Geräte, deren Betriebssysteme und die bereits vorhandenen Schutzmaßnahmen, werden am Beispiel der Tiroler Landeskrankenanstalten im **Kapitel 4** abgebildet.

Das **Kapitel 5** beschäftigt sich mit der Gegenüberstellung der möglichen Gefährdungen mit den möglichen Schutzmaßnahmen. Die Prüfung von den bereits im Einsatz befindlichen Schutzmaßnahmen ergibt ein Delta, welches durch zusätzliche Schutzmaßnahmen unterstützt werden kann. Daraus resultiert der Lösungsansatz zur Verminderung der möglichen Eintrittswahrscheinlichkeiten von Gefährdungen.

Im **Kapitel 6** werden die Resultate der einzelnen Betrachtungen zusammengefasst und ein Ausblick auf die weiteren Schritte gegeben.

2 Grundlagen

Im Grundlagen-Kapitel werden die Sicherheitsziele eines IT-Systems beschrieben. Des Weiteren werden die Themenbereiche allgemeine Gefährdungen und mögliche Fehlerursachen beschrieben. Eine weitere Betrachtung wert sind die möglichen Gefährdungen im Kontext mit dem OSI-Modell (Stein, 2008, S. 22). Weiters werden auch die rechtlichen Rahmenbedingungen behandelt.

2.1 Sicherheitsziele im Netzwerk

Im Allgemeinen versteht man unter den primären Sicherheitszielen der Computersicherheit die Vertraulichkeit, die Integrität und die Verfügbarkeit. Die Vertraulichkeit setzt dabei Authentizität voraus. Vor allem wenn man Kommunikationssicherheit hinzunimmt, sind weitere Sicherheitsziele zu definieren (Bumerl, 2010).

2.1.1 Vertraulichkeit (Confidentiality)

Vertraulichkeit bedeutet Schutz gegen unberechtigte Kenntnisnahme von gespeicherten, verarbeiteten oder übertragenen Informationen. Dies schließt auch den Schutz von Informationen ein, die für sich gesehen als "harmlos" erscheinen, aber dazu benutzt werden können, um Zugriff auf vertrauliche Informationen z.B. Systemkonfigurationsdaten zu erhalten.
In Rahmen der Kommunikationssicherheit kann das sogar bedeuten, dass selbst Wissen über das Stattfinden einer Kommunikation vertraulich bleiben soll (Bumerl, 2010).

2.1.2 Integrität (Integrity)

Integrität bedeutet die Sicherstellung der Korrektheit (Unversehrtheit, Richtigkeit und Vollständigkeit) von Informationen (Datenintegrität) bzw. der korrekten Funktionsweise von Systemen (Systemintegrität). An verarbeiteten, übertragenen oder gespeicherten Daten dürfen Modifikationen nur mit entsprechender Berechtigung und in beabsichtigter Weise vorgenommen werden (Bumerl, 2010).

2.1.3 Verfügbarkeit (Availability)

Alle verarbeiteten Daten, sowie die zur Verarbeitung notwendigen Systeme und Betriebsmittel, müssen jederzeit verfügbar, funktionsbereit bzw. in erwarteter und/ oder geforderter Qualität bereitstehen, wenn ein autorisierter Benutzer/ eine autorisierte Benutzerin darauf zugreifen will. Dies umfasst somit auch jegliche Hardware, Programme und Funktionen und schließt für Daten auch Archive und Sicherungskopien (Backups) mit ein (Bumerl, 2010).

2.1.4 Authentizität (Authenticity)

Authentizität bedeutet die Sicherstellung der Echtheit von Informationen bzw. die Sicherstellung der Echtheit der behaupteten Identität. Es muss einerseits sichergestellt sein, dass Informationen wirklich aus der angegebenen Quelle stammen (Nachrichtenauthentizität) bzw. dass die vorgegebene Identität, etwa eines Benutzers/ einer Benutzerin oder eines an der Kommunikation beteiligten Systems (Teilnehmerauthentizität) korrekt ist. Dieser notwendige Beweis kann durch unterschiedliche Mittel erbracht werden (Bumerl, 2010).

2.1.5 Verlässlichkeit (Reliability)

Verlässlichkeit bedeutet Schutz vor beabsichtigten oder unbeabsichtigten Störungen, beispielsweise durch Angriffe oder auch durch höhere Gewalt. Man kann in diesem Fall von der Verletzbarkeit eines Systems sprechen und diese wäre dann dem Punkt Verfügbarkeit zuzuordnen (Bumerl, 2010).

Die primären Sicherheitsmerkmale lassen sich sehr gut im C.I.A-Dreieck darstellen. Diese Darstellungsform wird in der Fachliteratur sehr gerne verwendet.

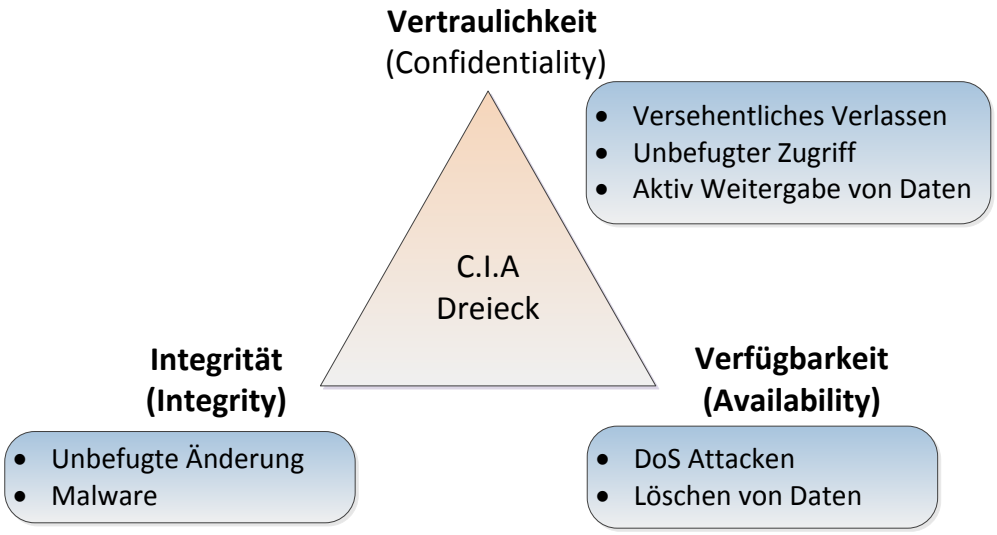

Abbildung 1: C.I.A-Dreieck (Microsoft, 2011, S. 122)

2.2 Sicherheitsaspekte des ISO-/ OSI-Modelles

2.2.1 Layer 1 – Physikalische Schichte

Die verwendeten Medien sind Kupferleitungen, Glasfaserleitungen, Licht in freier Ausbreitung und Funk durch Ausbreitung von elektromagnetischen Wellen.
Kupferleitungen können galvanisch oder induktiv leicht angezapft werden. Eine sichere Verlegung ist daher erforderlich, die EDV-Verteiler sind zu versperren und nur benutzte Netzwerkdosen sind zu patchen. Eine Abstrahlung der Leitungen durch fehlende Schirmung ist zu vermeiden.
Das Anzapfen von Glasfaserleitungen ist relativ schwierig, aber technisch möglich. Auch hier ist eine sichere Verlegung daher notwendig. Bei Licht in freier Ausbreitung und bei Funk ist das Abhören wegen der unkontrollierten Ausbreitung naturgemäß jederzeit möglich. Geeignete Schutzmaßnahmen wie z.B. Verschlüsselung sind daher unerlässlich (Eckert, 2009, S. 87).

2.2.2 Layer 2 – Verbindungsschichte

Auf Layer 2 (MAC-Layer) im Local Area Network (LAN) gibt es einige Möglichkeiten, den Netzwerkzugriff sicher zu gestalten. Bei Hubs (Multiport-Repeater) war dies noch nicht möglich, weil diese die Signale an allen Ports aussenden, aber durch die Verwendung von Switches wird die Sicherheit wesentlich erhöht. Diese senden die Pakete, mit Ausnahme der Broadcasts, nur zum Empfänger-Port aus. Dies setzt voraus, dass die Konfiguration richtig ist. Die Fernkonfigurationsmöglichkeit und das Netzwerk-Management-System (NMS) sind daher unbedingt abzusichern (z.B. wegen Port-Spiegelung). Per-Port-Switching erlaubt auch Port-Security, das bedeutet das Beschränken des Netzzuganges auf eine einzige, eventuell auch einige wenige, aufgelistete MAC-Adresse(n) an einem Port. Moderne Netzwerkswitches unterstützen die Authentifizierung und Autorisierung berechtigter Nutzer mittels IEEE 802.1x-Technik. Ein Netzwerkzugriff ist nur mit zentraler Benutzerverwaltung und mit Zertifikaten möglich (Stein, 2008, S. 29).

2.2.3 Layer 3 – Netzwerkschichte

Auf Layer 3 unterscheiden sich - im Hinblick auf das Internet – Local Area Network (LAN) und Wide Area Network (WAN) nicht mehr. Es wird das IP-Protokoll verwendet. Das Internet ist ein weltweites System zur Vermittlung von IP-Paketen zwischen allen TeilnehmerInnen. Die Rechner befinden sich meist in einem LAN. Diese LANs werden durch Anschluss an einen Internetprovider, der seinerseits wieder mit anderen Providern vernetzt ist, miteinander verbunden. So entsteht ein durchgängiges Vermittlungsnetz auf Layer 3 von Endgerät zu Endgerät. Es ist so gebaut, dass es blind Pakete vermittelt, wo immer das möglich ist. Die Absicherung der Paketweiterleitung ist vereinbarungsgemäß nicht Sache des Netzes, sondern Sache des Anwenders/ der Anwenderin. Auf Layer 3 kann eine Absicherung optimal angesetzt werden, weil hier das größte Gefährdungspotential besteht.

Alle Firewalls beschäftigen sich mit den diesbezüglichen Möglichkeiten. Es ist darauf zu achten, dass der Inhalt der Datenpakete selbst, deren Vermittlung und die Verwaltung der Vermittlung (Routingprotokolle) gesichert werden. Letzteres deshalb, weil die Signalisierung und Verwaltung im Internet inbound (nicht getrennt von den Nutzdaten) erfolgt. Es könnte der Inhalt der Pakete manipuliert werden, die Pakete könnten gezielt fehlgeleitet und/ oder abgehört werden oder die Routinginformationen könnten gefälscht werden, um die Datenvermittlung zu stören (Stein, 2008, S. 30).

2.2.4 Layer 4 – Transportschichte

Im Internet wird auf Layer 4 durch Portnummern sichtbar, welche Anwendung zwei Netzwerkpartner zu benutzen gedenken. Deshalb wird auch hier zur Erlangung sicherer Vernetzung eingegriffen. Man steuert, welcher Rechner über das Netz auf welchem Rechner welche Anwendungen benutzen darf. Weiters wird auf Layer 4 der Ablauf verbindungsorientierter Verbindungen (Transmission Control Protocol TCP) gesteuert und überwacht. Damit kann das Eindringen Dritter in bestehende Verbindungen verhindert werden (Man in the Middle-Attack). Verbindungslose Netzwerkprotokolle (User Datagram Protocol UDP) sind im Internet sehr problematisch und werden weitestgehend unterbunden, wenngleich sie durch Multimediaanwendungen immer mehr an Bedeutung erlangen (Stein, 2008, S. 31).

2.2.5 Layer 5 – Sitzungsschicht

Diese Schicht regelt die Prozesskommunikation zwischen zwei Systemen. Das RPC (Remote-Procedure-Call) stellt Dienste für einen sicheren Datenaustausch zur Verfügung.
Weiters regelt diese Schicht die Wiederherstellung einer verlorenen Sitzung. Eine Gefährdung stellt die unberechtigte Sitzungsübernahme nach einer Unterbrechung dar (Stein, 2008, S. 31).

2.2.6 Layer 6 – Darstellungsschicht

Die Darstellungsschicht ist für die korrekte Darstellung der Daten unter Verwendung eines normierten Zeichensatzes (z.B. ASCII) zuständig. Weitere Aufgaben stellen Datenkompression und Datenverschlüsselung dar. Eine nicht korrekte Darstellung von Daten durch Verwendung eines falschen Zeichensatzes ist jederzeit möglich (Stein, 2008, S. 32).

2.2.7 Layer 7 – Anwendungsschichte

Layer 3 und 4 können anhand der IP-Adressen und Portnummern nur steuern, welcher Rechner auf welchem anderen Rechner auf welche Applikationen zugreifen darf, nicht aber, welche Person oder welcher Prozess zugreifen darf.
Das IP-Netzwerk kennt nur die IP-Adressen und Portnummern der Kommunikationspartner, nicht aber die Identität von AnwenderInnen oder Prozessen.

Eine personenbezogene Absicherung kann nur auf der Anwendungsebene erfolgen, z.B. durch Username und Passwort, durch Karten, Zertifikate oder Codes. Hochwertige Sicherheitseinrichtungen haben auch Kenntnis von den Anwendungsprotokollen (ftp, HTTP, SMTP usw.) und können den korrekten Ablauf derartiger Übertragungen beurteilen. In diese Kategorie fallen auch die Systeme zur Abwehr schädigender Inhalte wie Virenscanner, SPAM-Filter usw (Stein, 2008, S. 32).

2.3 Rechtliche Grundlagen

2.3.1 Medizinproduktegesetz (MPG) und Medizinprodukte-Betreiberverordnung (MPBV)

Das österreichische Medizinproduktegesetz (MPG) ist am 1. Januar 1997 in Kraft getreten, die österreichische Medizinprodukte-Betreiberverordnung (MPBV) am 1. April 2007. Beide wurden durch das am 30. Dezember 2009 veröffentlichtes Bundesgesetz betreffend Medizinprodukte entsprechend den durch EU-Richtlinie 2007/47/EG geänderten EU-Richtlinien 90/385/EWG und 93/42/EWG modifiziert. Folgend werden Inhalte der Fassung vom 04.05.2011 des MPG bzw. der MPBV teils zusammenfassend angeführt:

Das Bundesgesetz (MPG) regelt die Funktionstüchtigkeit, Leistungsfähigkeit, Sicherheit und Qualität, die Herstellung, das Inverkehrbringen, den Vertrieb, das Errichten, die Inbetriebnahme, die Instandhaltung, den Betrieb, die Anwendung, die klinische Bewertung und Prüfung, die Überwachung und die Sterilisation, Desinfektion und Reinigung von Medizinprodukten und ihres Zubehörs sowie die Abwehr von Risiken und das Qualitätsmanagement beim Umgang mit Medizinprodukten und ihrem Zubehör.

Das Ziel ist, die Sicherheit, Eignung und Leistungsfähigkeit der Produkte sowie den Schutz vor allem gegenüber den PatientInnen, dem Personal sowie Dritten zu gewährleisten. Anstelle eines Zulassungsverfahrens sieht das MPG eine Zertifizierung der Produkte mit dem CE-Kennzeichen vor. Im Falle gesetzlicher Änderungen sind Hersteller von Produkten, die konform zum Medizinproduktegesetz sind, verpflichtet, die entsprechenden Anforderungen zu erfüllen und in Bezug auf ihre Produkte umzusetzen.

Medizinprodukte sind alle einzeln oder miteinander verbunden verwendeten Instrumente, Apparate, Vorrichtungen, Software, Stoffe oder anderen Gegenstände, einschließlich der vom Hersteller speziell zur Anwendung für diagnostische oder therapeutische Zwecke bestimmten und für ein einwandfreies Funktionieren des Medizinprodukts eingesetzten Software, die vom Hersteller zur Anwendung am Menschen bestimmt sind.

Medizinprodukte müssen so ausgelegt und hergestellt sein, dass ihre Anwendung weder den klinischen Zustand oder die Sicherheit der PatientInnen noch die Sicherheit der AnwenderInnen oder Dritter gefährdet, wenn sie unter den vorgesehenen Bedingungen und zu den vorgesehenen Zwecken eingesetzt werden.

Etwaige Risiken und Nebenwirkungen, die bei bestimmungsgemäßer Installation, Implantation oder Anwendung auftreten können, müssen unter Berücksichtigung der Wirksamkeit der Medizinprodukte nach dem Stand der medizinischen Wissenschaften und der Technik vertretbar sein und der Schutz der Gesundheit und Sicherheit muss gewährleistet sein.

Medizinprodukte mit Ausnahme von Sonderanfertigungen, Medizinprodukten gemäß § 32, für die klinische Prüfung bestimmten Medizinprodukten sowie In-vitro-Diagnostika für Leistungsbewertungszwecke dürfen nur dann in Verkehr gebracht und in Betrieb genommen werden, wenn sie mit der CE-Kennzeichnung gemäß diesem Bundesgesetz oder auf der Grundlage der Richtlinien 90/385/EWG, 93/42/EWG und 98/79/EG ergangenen nationalen Vorschriften anderer Vertragsparteien des Abkommens über den Europäischen Wirtschaftsraum versehen sind.

Der Bundesminister für Gesundheit und Konsumentenschutz hat durch Verordnung im Hinblick auf die Zweckbestimmung, die eingesetzte Technologie sowie auf Anwendungsort, -art und -dauer der Medizinprodukte unter Bedachtnahme auf die einschlägigen Rechtsakte der Europäischen Gemeinschaften

1. jene Klassen festzulegen, denen Medizinprodukte insbesondere im Hinblick auf die Konformitätsbewertung zuzuordnen sind, und
2. die Kriterien und Regeln festzulegen, nach denen Medizinprodukte den Klassen zuzuordnen sind.

Angehörige eines gesetzlich geregelten Gesundheitsberufes, Gewerbeberechtigte, die berufsmäßig zum Betreiben oder zur Anwendung eines Medizinproduktes befugt sind, Leiter von einschlägigen Prüf-, Inspektions- und Zertifizierungsstellen und technische Sicherheitsbeauftragte von Krankenanstalten haben Informationen über Medizinprodukte im Hinblick auf Zwischenfälle, insbesondere

1. jede Fehlfunktion oder jede Änderung der Merkmale oder der Leistung eines Medizinproduktes sowie jeden Mangel in Bezug auf die Kennzeichnung oder die Gebrauchsanweisung, die geeignet sind, zum Tod oder zu einer schwerwiegenden Verschlechterung des Gesundheitszustandes eines Patienten/ einer Patientin, eines Anwenders/ einer Anwenderin oder eines/r Dritten zu führen oder die dazu geführt hat, oder
2. bisher unbekannte schwerwiegende Nebenwirkungen oder das vermehrte Auftreten bekannter schwerwiegender Nebenwirkungen, oder
3. bisher unbekannte wechselseitige Beeinflussungen, oder
4. schwerwiegende Qualitätsmängel,

die ihnen aufgrund ihrer beruflichen Tätigkeit bekanntgeworden sind, unverzüglich dem Bundesamt für Sicherheit im Gesundheitswesen zu melden sowie alle Beobachtungen und Daten mitzuteilen, die für die Medizinproduktesicherheit von Bedeutung sein können.
Meldungen haben bei Krankenanstalten, außer bei sonstiger Gefahr im Verzug, einheitlich im Wege des ärztlichen Leiters zu erfolgen.

Das Hauptstück V des MPG bezieht sich auf die Vorschriften für das Errichten, Betreiben, Anwenden und Instandhalten von Medizinprodukten inner- und außerhalb von Einrichtungen des Gesundheitswesens. Dies wird in der folgenden MPBV angeführt und entfällt an dieser Stelle.

Durch die MPBV wird die Instandhaltung von Medizinprodukten in österreichischen Einrichtungen des Gesundheitswesens detailliert geregelt. Der Großteil dieser Reglungen ist nicht neu, da diese bereits im Medizinproduktegesetz (BGBl.-Nr. 657/1996) enthalten sind. Die MPBV stellt daher eine Präzisierung des MPG dar.

Die MPBV gilt für das Errichten, Betreiben, Anwenden und Instandhalten von Medizinprodukten in Einrichtungen des Gesundheitswesens.

Der Betreiber hat vor der erstmaligen Anwendung eines kritischen Medizinproduktes am Betriebsort eine Eingangsprüfung durchzuführen oder durchführen zu lassen. Die kritischen Medizinprodukte sind im Anhang 1 der MPBV aufgelistet.

Der Umfang der Eingangsprüfung hat sich am Prüfumfang der wiederkehrenden sicherheitstechnischen Prüfung (STK) zu orientieren. Der bestellte Technische Sicherheitsbeauftragte (TSB) hat das Recht, zusätzliche, über Anhang 1 hinausgehende, Medizinprodukte (MP) zu benennen, für die eine verpflichtende Eingangsprüfung durchzuführen ist.

Der Betreiber hat sicherzustellen, dass jede mit der Handhabung eines Medizinproduktes befasste Person eingewiesen wird. Im Gegensatz zu Deutschland wurde in Österreich das sogenannte "Schneeballsystem", bei dem eingeschulte Personen ihrerseits wiederum Einschulungen durchführen können, nicht untersagt.

Von einer Einweisung ausgenommen sind lediglich Personen, bei denen aufgrund ihrer Ausbildung, ihrer sonstigen Kenntnisse oder praktischen Erfahrungen davon ausgegangen werden kann, dass ihnen diese Informationen hinlänglich bekannt sind.
Für alle kritischen Medizinprodukte nach Anhang 1 und für solche, die vom TSB dazu nominiert wurden, ist die Einweisung zu dokumentieren.

In bestimmten Fällen, wie etwa bei Anmeldung eines Einweisungsbedarfs durch den Anwender selbst oder bei wiederholten Bedienungsfehlern, nach Software-Updates oder bei Änderungen des Anwendungs- oder Einsatzbereiches, können auch wiederkehrende Einweisungen erforderlich werden. Der detaillierte Inhalt der Einweisungen und die zu dokumentierenden Daten können der MPBV entnommen werden.

Der Betreiber ist verpflichtet, die in seiner Einrichtung in Verwendung stehenden Medizinprodukte instandzuhalten. Die Instandhaltung ist unter Berücksichtigung der Herstellerangaben so vorzunehmen, dass die Sicherheit von PatientInnen, AnwenderInnen und Dritten nicht gefährdet wird.

Der Betreiber hat bei allen aktiven (nicht implantierbaren) Medizinprodukten eine sicherheitstechnische Prüfung (STK) vorzunehmen oder vornehmen zu lassen. Dies gilt auch für nichtaktive Medizinprodukte, wenn dies der Hersteller angibt. Ausgenommen sind lediglich unkritische, batteriebetriebene Medizinprodukte, die nicht vom Anhang 1 erfasst sind und auch nur dann, wenn eine STK nicht explizit vom Hersteller gefordert wird.

Die STK ist hinsichtlich Prüfumfang und Prüfintervall nach den Herstellerangaben durchzuführen. Der TSB darf in begründeten Fällen das Prüfintervall reduzieren oder den Prüfumfang vergrößern, muss dies aber dokumentieren. Wenn der Hersteller eine STK dezidiert ausschließt, so ist zumindest eine Sichtprüfung vorzunehmen. Bei fehlenden Angaben des Herstellers für Prüfumfang und -Intervall, sind Letztere nach dem Stand der Technik festzulegen, wobei auch eine Kontrolle aller sicherheitsrelevanten Funktionen enthalten sein muss. Die Regelungen für die STK gelten auch für Systeme und Behandlungseinheiten, also auch für zusammengesetzte oder gekoppelte Medizinprodukte. Über die STK ist ein Protokoll anzufertigen. Die aufzunehmenden Mindestdaten sind der MPBV zu entnehmen. Die Prüfprotokolle sind fünf Jahre aufzubewahren.

Der Betreiber hat bei allen Medizinprodukten nach Anhang 2 sowie bei Medizinprodukten, für die der Hersteller solche Kontrollen vorgesehen hat, eine MTK (Messtechnische Kontrolle) zum Zwecke der Rückführung auf nationale oder internationale Normen durchzuführen oder durchführen zu lassen.
Bei der MTK sind die vom Hersteller angegebenen Fehlergrenzen zugrunde zu legen. Liegen keine Herstellerangaben vor, so gelten die Angaben in Normen oder nach dem Stand der Technik. Es gelten die vom Hersteller angegebenen Intervalle bzw. bei Fehlen derselben die im Anhang 2 genannten Intervalle. Schließt der Hersteller eine MTK explizit aus, so ist sie nur bei Anzeichen auf Nichteinhaltung der Fehlergrenzen oder bei Beeinflussung der Messeigenschaften durchzuführen. In diesen Fällen ist eine MTK unverzüglich durchzuführen.

In die Gerätedatei sind alle STK- und MTK-pflichtigen Medizinprodukte aufzunehmen. Ausgenommen sind manuelle Blutdruckmessgeräte, batteriebetriebene Lichtquellen, nicht zur Überwachung verwendete Pulsmessgeräte und elektrische Fieberthermometer.
Der Betreiber hat eine/n Verantwortliche/n zum Führen der Gerätedatei zu bestimmen. Für die Gerätedatei sind alle Datenträger inklusive Papierform zulässig, wenn die Daten während der geforderten Aufbewahrungsdauer verfügbar sind. Die Mindestinhalte der Gerätedatei sind in der MPBV aufgelistet.
Sie muss während der Betriebszeit zugänglich sein. Nach Außerbetriebnahme eines Medizinproduktes müssen dessen Daten noch für weitere fünf Jahre verfügbar sein.

Der Betreiber hat für alle zur Verwendung bereitstehenden aktiven MP ein Bestandsverzeichnis zu führen, welches auch mit der Gerätedatei gemeinsam geführt werden darf.
Die Inhalte des Bestandsverzeichnisses können der MPBV entnommen werden. Im Übrigen gelten die analogen Anforderungen wie für die Gerätedatei.

Der Betreiber hat für alle implantierbaren Medizinprodukte nach Anhang 5 ein Implantat-Register zu führen:
Für das Implantat-Register sind alle Datenträger inklusive der Papierform zulässig, wenn sie die Verfügbarkeit für die Aufbewahrungsdauer gewährleisten.

Durch die MPBV wird die Instandhaltung von Medizinprodukten in österreichischen Einrichtungen des Gesundheitswesens detailliert geregelt. Der Großteil dieser Regelungen ist nicht neu, da diese bereits im Medizinproduktegesetz (BGBl.-Nr. 657/1996) enthalten sind. Die MPBV stellt daher eine Präzisierung des MPG dar.

2.3.2 IEC-Norm 80001 „Risikomanagement vernetzter Medizinprodukte“

Folgende Ausführungen bzw. Inhalte sind an Gärtner (Gärtner, Medizinische Netzwerke und Software als Medizinprodukt, Band 5, 2010) angelehnt:
Die IEC 80001 richtet sich sowohl an Hersteller als auch an Betreiber, die Aufgaben und Verantwortlichkeiten definieren müssen, und liegt derzeit als Entwurf vor. Ein wesentliches Thema ist sowohl die Einführung eines Risikomanagements bevor ein Medizinprodukt an ein IT-Datennetzwerk anschlossen wird, als auch, dass dies über den gesamten Lebenszyklus betrieben wird. Das Ziel ist, unerwünschte Auswirkungen, die zum Schaden an PatientInnen führen können, zu verhindern.

Folgende Ziele sollen mit der neuen Norm erreicht werden:

- Sicherheit im Netzwerk
- Effektives Netzwerk
- Daten- und Systemsicherheit
- Vertraulichkeit, Integrität und Verfügbarkeit von Daten
- Interoperabilität
- Zusammenschaltung von Medizinprodukten und Geräten, welche keine Medizinprodukte sind, im selben IT-Netzwerk.

Für die Zielerreichung ist es einerseits notwendig, dass die Leistungsmerkmale des IT-Netzwerkes definiert werden, und andererseits, dass der Hersteller im Rahmen von Vereinbarungen die benötigten Informationen zur Verfügung stellt. Seitens des Betreibers ist ein Risikomanager zu benennen, welcher sich um das Risikomanagement und um die Integration von Medizinprodukten kümmert.

In der IEC 80001-Norm sind die Aufgaben des Betreibers (oberste Leitung, Risikomanager, etc.), die Aufgaben und Pflichten des Herstellers sowohl für Medizinprodukte als auch für IT-Komponenten angeführt. Im Detail wird dies in dieser Arbeit nicht ausformuliert.

2.3.3 DIN EN 60601-1-3rd „Medizinische elektrische Geräte“

Folgende Ausführungen bzw. Inhalte sind an (Gärtner, Elektrische Sicherheit in der Medizintechnik, 2008) angelehnt:
Die dritte Ausgabe der DIN EN 60601-1 „Medizinische elektrische Geräte“ ist im Juli 2007 in Kraft getreten und gilt für die Basissicherheit und die Leistungsmerkmale von medizinischen elektrischen Geräten und Systemen mit einem Anschluss an ein Versorgungsnetz, das zur Diagnose, Behandlung oder Überwachung eines Patienten/ einer Patientin nach Herstellerangaben bestimmt ist.

Durch die zunehmende Vernetzung, und somit Integration von Medizintechnikprodukten in IT-Netzwerke des Betreibers, fordert die DIN EN 60601-1 die Funktion/ Position eines Systemintegrators oder Netzwerkverantwortlichen.

Die folgende Klasseneinteilung des IT-Netzwerkes, an welches Medizinprodukte angeschlossen sind, wäre möglich:

- Das IT-Netzwerk der Klasse A ist das allgemeine Kliniknetzwerk und umfasst sämtliche administrativen Applikationen.
- Das IT-Netzwerk der Klasse B kann z.B. ein radiologisches Netzwerk sein, das einen eingeschränkten bzw. kontrollierten Zugang (z.B. über ein Gateway) in das Klasse A-IT-Netzwerk hat.
- Das IT-Netzwerk der Klasse C kann z.B. ein Intensivmedizinisches Netzwerk sein und das ist von allen anderen IT-Netzwerken getrennt.

2.3.4 DIN ISO/ IEC 27001 „Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen

Folgende Ausführungen sind der DIN ISO/ IEC 27001 entnommen bzw. an diese angelehnt. Die in dieser internationalen Norm festgelegten Anforderungen sind allgemeiner Natur und auf alle Organisationen anwendbar - unabhängig von Art, Größe und Beschaffenheit.

Diese Norm wurde entwickelt, um ein Modell und einen prozessorientierten Ansatz für die Einrichtung, Umsetzung, Durchführung, Überwachung, Überprüfung, Instandhaltung und Verbesserung eines Informationssicherheits-Managementsystems (ISMS) bereitzustellen und betont die Wichtigkeit der folgenden Punkte für seine AnwenderInnen:

- Verständnis der Anforderungen der Organisation an Informationssicherheit und die Notwendigkeit, eine Leitlinie und Ziele für Informationssicherheit festzulegen;
- Umsetzung und Betrieb von Maßnahmen, um die Informationssicherheitsrisiken einer Organisation in Zusammenhang mit den allgemeinen Geschäftsrisiken der Organisation zu verwalten;

- Überwachung und Überprüfung der Leistung und Wirksamkeit des ISMS und
- ständige Verbesserung auf der Basis von objektiven Messungen.

Es wird das „Plan-Do-Check-Act“-Modell (PDCA – Planen, Durchführen, Prüfen, Handeln) verwendet, um die ISMS-Prozesse zu strukturieren.

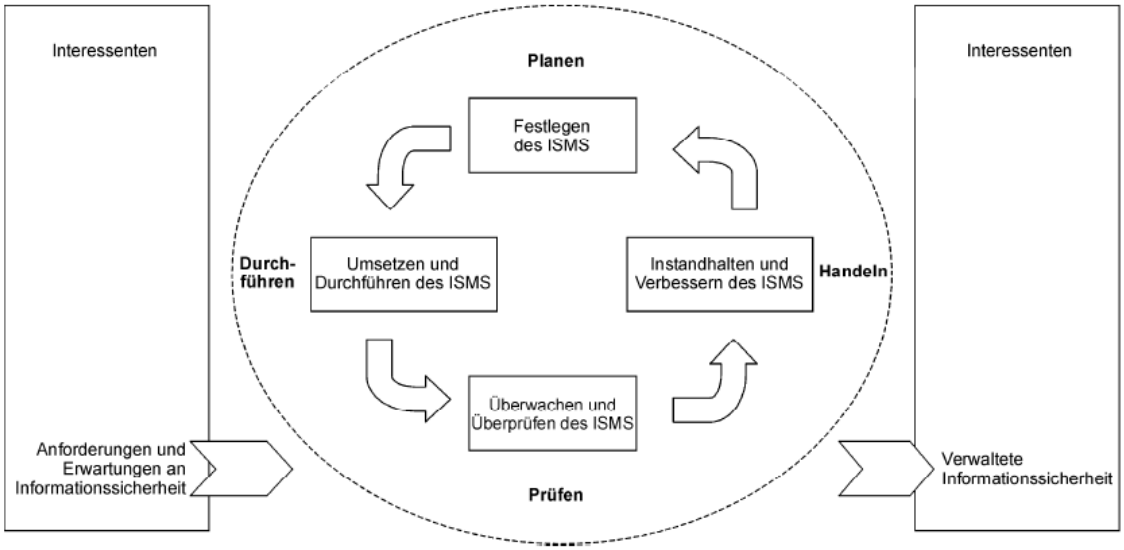

Abbildung 2: PDCA nach DIN ISO/IEC 27001

Planen (Festlegen des ISMS): Festlegen der ISMS-Leitlinie, -Ziele, -Prozesse und -Verfahren, die für das Risikomanagement und die Verbesserung der Informationssicherheit notwendig sind, um Ergebnisse im Rahmen aller Grundsätze und Ziele einer Organisation zu erreichen.

Durchführen (Umsetzen und Durchführen des ISMS): Umsetzung und Durchführung der ISMS-Leitlinie, -Maßnahmen, -Prozesse und -Verfahren.

Prüfen (Überwachen und Überprüfen des ISMS): Einschätzen und ggf. Messen der Prozessleistung an der ISMS-Leitlinie, den ISMS-Zielen und praktischen Erfahrungen, und Berichten der Ergebnisse an das Management zwecks Überprüfung.

Handeln (Instandhalten und Verbessern des ISMS): Ergreifen von Korrektur- und Vorbeugungsmaßnahmen - basierend auf den Ergebnissen von internen ISMS-Audits - und Überprüfungen des Managements und anderer wesentlicher Informationen, zur ständigen Verbesserung des ISMS.

2.4 Gefährdungskategorien

Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) beschäftigt sich mit dem Thema Informationssicherheit und dem primären Ziel von sicherem Einsatz von Informations- und Kommunikationstechnik in unserer Gesellschaft.
Sehr viele Arbeitsprozesse werden im Gesundheitswesen durch integrierte Informationssysteme unterstützt. Der einwandfreie Betrieb dieser Systeme, insbesondere in Kombination mit der Medizintechnik, ist von essentieller Bedeutung für den Krankenhausbetrieb.
Das Bundesamt für Sicherheit in der Informationstechnik (BSI Grundschutz, 2011) unterteilt die möglichen Gefährdungen in folgende Themenbereiche:

2.4.1 Höhere Gewalt

Unter höherer Gewalt versteht man ein von außen kommendes, unvorhersehbares Ereignis, welches auch durch möglichste Sorgfalt nicht verhindert werden kann.
Typische Beispiele für höhere Gewalt sind Blitz, Feuer, Hochwasser, Sturm, Terrorismus oder Erdbeben.
Dies betrifft auch den Ausfall von externen Versorgungseinrichtungen wie Stromversorgung, Daten- und Funknetze und Telekommunikationseinrichtungen
(BSI Grundschutz, 2011).

2.4.2 Organisatorische Mängel

Durch unzureichende Planung von betrieblichen Abläufen und Prozessen entstehen sehr oft organisatorische Mängel, welche sich in den verschiedensten Themenbereichen der IT-Sicherheit niederschlagen können. Fehlende Notfallplanung und Wiederanlaufkonzepte des Rechenzentrums können bei Ausfällen zu drastischen Betriebsbeeinträchtigungen führen (BSI Grundschutz, 2011).
Organisatorische Änderungen im Bereich Personal, Betriebsführung und Technik, welche wesentlichen Einfluss auf die Informationssicherheit haben, werden oft nicht an die neuen Gegebenheiten angepasst.
Ein Klassiker ist zum Beispiel die fehlende Sperre der User-Rechte bei Austritt von MitarbeiterInnen (BSI Grundschutz, 2011).

2.4.3 Menschliche Fehlhandlungen

Durch menschliches Fehlverhalten können Schäden aus Unwissenheit oder Böswilligkeit entstehen. Das Bundesamt für Sicherheit in der Informationstechnik versteht unter menschlichen Fehlhandlungen unwissentlich durchgeführte Konfigurations- und Bedienungsfehler. Die Vertraulichkeit und die Integrität von Daten werden durch menschliches Fehlverhalten oft verletzt. Unbeabsichtigtes Löschen von Daten und Programmen und/ oder fehlende Datensicherung führen oft zu Datenverlusten. Fehlkonfigurationen von IT-Systemen stellen oft eine große sicherheitstechnische Gefährdung dar.

Vorsätzliches Fehlverhalten wird in der Kategorie „Vorsätzliche Handlungen“ eigens behandelt (BSI Grundschutz, 2011).

2.4.4 Technisches Versagen

Technisches Versagen entspricht dem Fehlverhalten von Hard- bzw. Softwarekomponenten und den dazugehörigen Versorgungseinheiten wie Stromversorgung und Klimatisierung. Fehleranfällige Hard- und Softwarekomponenten, komplexes Design der Systeme, geringe Fehlertoleranz und fehlende Backupsysteme führen häufig zu Defekten.
Eine IT-Infrastruktur, welche nicht dem Stand der Technik entspricht, stellt für einen sicheren Betrieb eine große Gefahr dar (BSI Grundschutz, 2011).

2.4.5 Vorsätzliche Handlungen

Aus unterschiedlichsten Beweggründen (Spionage, Böswilligkeit, Frust, usw.) können durch vorsätzliche Handlungen IT-Systeme und deren Daten manipuliert oder zerstört werden. Dies kann eine unerlaubte Einsichtnahme in vertrauenswürdige Daten oder eine absichtliche Infizierung mit Schadsoftware sein.
Der Täterkreis umfasst sowohl sogenannte Innentäter (MitarbeiterInnen der eigenen Organisation) als auch externe Täter (AußentäterInnen), beide Täterkreise stellen Bedrohungen für die IT-Systeme dar.
Die größten Gefahren für die IT-Systeme stellen demnach Naturkatastrophen, Ausfall von Technik, Softwarefehler, unwissentliches menschliches Versagen, fehlende Schutzeinrichtungen und organisatorische Mängel dar (BSI Grundschutz, 2011).

2.5 **Angriffsformen**

Die verschiedensten Arten von externen Bedrohungen werden in den folgenden Abschnitten behandelt.
In einer Kommunikationsbeziehung zwischen zwei Instanzen (Quelle und Senke) existieren im Allgemeinen verschiedene Bedrohungsszenarien.
Hört ein Angreifer die Datenverbindung zwischen Quelle und Senke ab, so können die gesendeten Nachrichten mitgelesen und auch die Kommunikationsbeziehungen analysiert werden. Wird die Datenübertragung ohne Verschlüsselungstechnologien durchgeführt, so können Informationen ohne großen technischen Aufwand an unberechtigte Dritte weitergegeben werden.
Kann der Angreifer zusätzlich die Nachrichten für seine eigenen Zwecke manipulieren, so ist er in der Lage, beide Kommunikationspartner zu beeinflussen. Die Daten können gelöscht, verändert oder auch zusätzliche Daten übertragen werden.
Aus diesen Gründen wird zwischen >>passiven<< und >>aktiven<< Angriffen unterschieden (Pohlmann & et al., 2006, S. 44).

2.5.1 Passive Angriffe

Der passive Angriff, auch Abhören genannt, erfolgt ohne Veränderung der zu übertragenden Daten bzw. Informationen. Durch das Abhören wird der Betrieb des IT-Systems normalerweise nicht beeinträchtigt. Je nach Art des physikalischen Übertragungsmediums unterscheidet sich der technische Aufwand. Eine analoge Telefonverbindung oder ein ungesichertes Wireless-LAN ist zum Beispiel sehr leicht abzuhören, eine optische Glasfaserverbindung jedoch ist nur mit hohem technischem Aufwand abhörbar. Eine Duplizierung der Datenströme (port mirroring) auf Netzwerkkomponenten ist eine sehr gängige und einfache Art zur Durchführung von passiven Angriffen. Unter anderem werden nicht nur Nutzdaten sondern auch gerne Passwörter oder Zugangsberechtigungen in Erfahrung gebracht (Pohlmann & et al., 2006, S. 45).

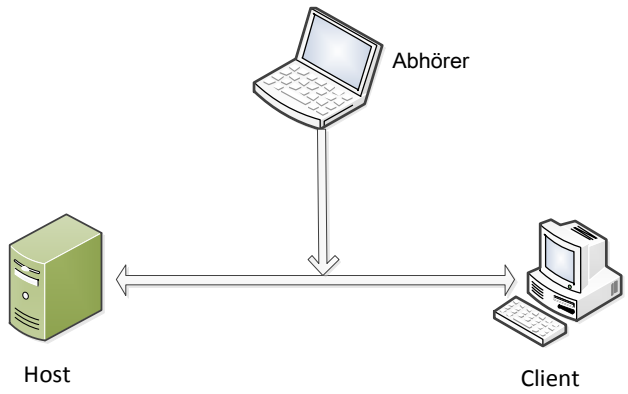

Abbildung 3: Passiver Angriff

2.5.2 Aktive Angriffe

Im Unterschied zum passiven Abhören können in diesem Falle Daten eingefügt, gelöscht oder verändert werden. Typischerweise setzt sich der Angreifer mittels Hard- oder Softwarekomponenten zwischen die KommunikationsteilnehmerInnen und kann dadurch die Datenströme für seine eigenen Zwecke missbrauchen (Pohlmann & et al., 2006, S. 48).

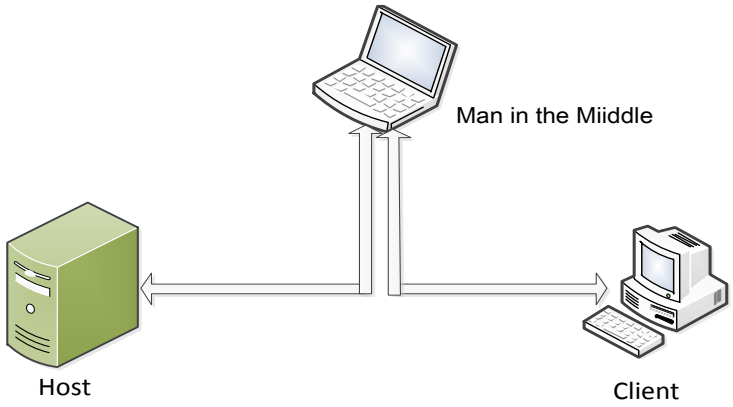

Abbildung 4: Aktiver Angriff

Aktive Angriffe werden auch „Man in the Middle“ oder „Mallory“ genannt und typische Arten dieser Angriffe sind:

- Dienst- und Kommunikationsunterbrechung (Denial of Service)
- Nachrichtenverzögerung
- Wiederholungsangriffe
- Nachrichtenverfälschung
- Kombinatorische Angriffe

Dienst- und Kommunikationsunterbrechung

Eine der bekanntesten Art der aktiven Gefährdungen ist die Dienst- oder Kommunikationsunterbrechung. Diese Angriffsart wird oft mit dem bekannten Namen Denial of Service (DoS) bezeichnet. Rechner, Server oder ganze Netzwerke werden mit Verbindungsversuchen überflutet, sodass in der Folge IT-Services nicht mehr zur Verfügung stehen können.
Eine besonders böswillige Form dieser DoS-Attacken sind die sogenannten „Distributed Denial of Service“ kurz DDoS-Attacken. Über Schadsoftware werden DDoS-Programme auf den verschiedensten internen und externen Rechnern eingeschleust und installiert. In Summe bilden diese Rechner ein sogenanntes Bot-Netzwerk, um gezielte Angriffe auf Systeme durchführen zu können (Pohlmann & et al., 2006, S. 50).

Die DoS-Attacken können in folgende Klassen eingeteilt werden:

- Physikalischer Angriff
- Ausnutzung von Implementierungsschwächen
- Ausnutzung von Protokollschwächen
- Erzeugung von Ressourcenmangel

Typisches Beispiel für diese Angriffsart ist die Störung von Webservern. Dabei werden einzelne Websites so oft aufgerufen, dass das Serversystem komplett ausgelastet ist und keine neuen Anfragen mehr entgegennehmen kann und aus diesem Grund ist die Website nicht mehr erreichbar. Ein weiteres Beispiel ist das Abfangen von Alarmmeldungen durch gezielte Kommunikationsunterbrechungen.

Nachrichtenverzögerung

Beabsichtigte Verzögerung von Nachrichten bewirkt in zeitkritischen Systemen die Hemmung von Kommunikationsflüssen bis zur vollständigen Blockade. Dazu nutzt der Angreifer den gezielten Einsatz von verschiedenen Protokollen, um das Timingverhalten der IT-Services zu stören. Diese Beeinflussung stellt in Echtzeitsystemen eine besondere Gefahr dar.
Laut Definition von Herrn Beierlein (Beierlein & et al., 2004, S. 338) ist ein Echtzeitsystem ein System, welches explizit vorgegebene endliche Fristen einhalten muss oder ansonsten ernsthafte Konsequenzen, inklusive Fehlfunktionen, riskiert.
Von harter Echtzeit spricht man, wenn eine Verletzung der geforderten zeitlichen Spezifikation zu ernsthaften Fehlfunktionen, bis zum Totalausfall, führt. Ein typisches Beispiel ist eine Joy-Stick-Steuerung eines OP-Roboters.
Unter weicher Echtzeit versteht man Situationen, in denen eine Verletzung der geforderten Reaktionszeit keine katastrophalen Auswirkungen hat. Dies führt zu einer Minderung der Leistungsfähigkeit des Systems. Ein typischer Vertreter dieser Störung wäre eine verzögerte Zustellung eines Laborbefundes oder eines Röntgenbefundes (Pohlmann & et al., 2006, S. 50).

Wiederholungsangriffe

Ein Wiederholungsangriff (auch Replay-Attacke genannt) besteht darin, bereits abgehörte Datenpakete mit derselben oder mit einer falschen Identität wieder erneut zu senden. Diese Angriffsart hat keinen Einfluss auf den eigentlichen Kommunikationsvorgang. Als Beispiel kann hier die mehrfache Übertragung von einem Überweisungsauftrag genannt werden (Pohlmann & et al., 2006, S. 50).

Nachrichtenverfälschung

Bei dieser Angriffsform werden Daten absichtlich manipuliert, Kommunikationsprotokolle nachhaltig verändert und auch letztlich IT-Services gestört.
Ein typisches Beispiel ist hier die Übernahme einer aktiven Kommunikationsverbindung nach einem erfolgreichen Login in ein System, das sogenannte session-highjacking. In diesem Fall übernimmt ein Unberechtigter die Session eines berechtigten Users.

Kombinatorische Angriffe

Die Angriffsmöglichkeiten werden immer häufiger miteinander kombiniert, um die Sicherheitsziele zu gefährden. Beispielsweise wird ein IT-Service durch eine DoS-Attacke gestört, um anschließend durch eine „Man in the Middle-Attacke“ eine Nachrichtenverfälschung durchzuführen (Bless, 2005, S. 18).

2.6 Fehlerquellen

Neben der Gefährdung durch aktive und passive Angriffe können IT-Systeme auch durch menschliche Fehlleistungen, technisches Versagen oder durch höhere Gewalt in Bezug auf die erforderlichen Sicherheitsziele gefährdet werden.

2.6.1 Übertragungsfehler

Die Übertragung von Daten kann durch verschiedenste Einflüsse wie z.B. durch Übersprechen auf Kupferleitungen manipuliert werden. Eine besondere Herausforderung stellt die Übertragung der Daten auf Funkbasis dar. Spezielle Übertragungsverfahren und Fehlerkompensationsmethoden sind für die korrekte Übertragung der Daten notwendig. Durch neue Übertragungsverfahren können auch zeitkritische Daten wie Sprache und Video auf qualitativ schlechten Leitungen übertragen werden
(Pohlmann & et al., 2006, S. 52).

2.6.2 Softwarefehler

Programmfehler oder Softwarebugs bezeichnen das Fehlverhalten von Programmen. Jedes Softwarepaket wird von Menschen erstellt und das fehlerfreie Funktionieren dieser Applikationen hängt natürlich von der Kompetenz des jeweiligen Programmierers bzw. der Qualitätssicherung ab. Fehler in der Syntax, Laufzeitprobleme oder Fehler in der Programmlogik führen zu Fehlverhalten bei den eingesetzten Applikationen. Aus diesen Gründen ist es notwendig, eine Qualitätssicherung bei der Erstellung der Software zu gewährleisten. Zudem stellt der Zeitdruck beim Erstellen eines fehlerfreien Programmcodes eine besondere Herausforderung dar. Spezielle Programme, sogenannte Debugger-Programme, können bei der Fehlerbehebung sehr hilfreich sein.

Aus diesen Gründen ist davon auszugehen, dass keine fehlerfreie Software im Einsatz ist und daher mit Fehlfunktionen der Software zu rechnen ist. Die Auswirkungen können geringe bis fatale Folgen, wie zum Beispiel eine überhöhte Dosis bei der Bestrahlung von PatientInnen, haben (Eckert, 2009, S. 15).

2.6.3 Hardwarefehler

Jede Hardware hat eine begrenzte Lebensdauer im laufenden Betrieb. Alterung der Bauelemente und auch Störungen von mechanischen Komponenten wie Festplatten und Lüftern führen oft zu Ausfällen. Die Fehleranfälligkeit ist nach der ersten Inbetriebnahme der Systeme (Kinderkrankheiten) und am Ende der möglichen Einsatzdauer am größten. Fehlverhalten in der elektrischen Versorgung, wie Überspannung und Spannungsspitzen, können zu Störungen der Systeme führen. Hohe Umgebungstemperaturen, Erschütterungen, Staub usw. können den reibungslosen Betrieb der Systeme gefährden. Aus diesen Gründen sind die geforderten Rahmenbedingungen der Hersteller für den sicheren Einsatz der Hardware zu garantieren (Pohlmann & et al., 2006, S. 54).

2.6.4 Umwelteinflüsse

Blitzschläge verursachen Überspannungen und Spannungsspitzen in den elektrischen Kommunikations- und Versorgungsnetzen. Durch magnetische Störungen können sowohl Funknetze in der Datenübertragung als auch IT-Systeme beträchtlich gestört werden. Die korrekte und fehlerfreie Übertragung der Kommunikationsdaten stellt bei Funknetzen eine besondere Herausforderung dar. Transformatorstationen können durch ihre große magnetische Strahlung angrenzende IT-Systeme in der Funktion gefährden.

2.6.5 Fehlbedienung

Bei Bedienungsfehlern handelt es sich um ein Fehlverhalten des Benutzers/ der Benutzerin, welches durch Unwissenheit oder durch fehlende Konzentration hervorgerufen werden kann. Bedienungsfehler können durch gezielte Schulung der BenutzerInnen oder durch spezielle Sicherheitsvorsorgen in der Applikation minimiert werden. Oft sind unzureichende Hilfen in der Software und fehlende oder nicht aktuelle Benutzerhandbücher vorhanden.

2.7 **Schadsoftware**

Mit dem Begriff Schadsoftware („Malware“ – **Mal**icious Soft**ware**) bezeichnet man Computerprogramme, welche entwickelt wurden, um unerwünschte oder schädliche Funktionen auszuführen. Die BenutzerInnen dulden im Normalfall keine schädliche Softwareapplikationen auf den Systemen und daher laufen diese meistens getarnt im Hintergrund.
Die Folge kann eine Löschung oder Manipulation von Daten sein oder das System wird in seiner Funktion nachhaltig gestört. Weiters können Sicherheitseinrichtungen kompromittiert werden, sodass Schadsoftware installiert werden kann.
Eine Deinstallation von Schadsoftware ist meistens mit den üblichen Deinstallationsroutinen nicht möglich und es wird daher eine spezielle Software benötigt.
In den folgenden Unterkapiteln werden die verschiedenen Arten der meistverbreiteten Schadsoftwaren beschrieben (Kaspersky, 2008, S. 50).

2.7.1 Computerviren

Als Viren werden Programme bezeichnet, welche sich als Bestandteil in Anwendungsdaten (Wirten) installieren und bei deren Verwendung in weitere Anwendungsdaten hineinkopieren. Die Vermehrung wird durch Ausführung des schadhaften Codes durchgeführt und die Verbreitung geschieht über elektronischen Datenaustausch oder durch Übertragung mittels mobilen Datenträgern wie z.B. USB-Sticks. Neben der Minimalfunktion der Vermehrung der Schadsoftware kann es von einer Manipulation der Daten bis hin zur Löschung der Daten kommen und auch Softwareapplikationen können in deren Funktion nachhaltig gestört werden. Eine spezielle Variante ist der Makrovirus, welcher Makro-Sprachen verschiedener Hersteller benutzt, um Schaden anzurichten (Kaspersky, 2008, S. 56).

2.7.2 Computerwurm

Als Computerwürmer werden Computerviren bezeichnet, welche sich selbstständig über IT-Datennetzte und im Speziellen über das Internet verbreiten können. Computerwürmer können sich z.B. über E-Mail-Systeme verbreiten und können sogar gesamte IT-Datennetzte lahmlegen. Diese Art von Schadsoftware kann natürlich einen größeren wirtschaftlichen Schaden anrichten als ein „normaler“ Virus (Kaspersky, 2008, S. 53).

2.7.3 Trojaner

Trojaner sind Programme, welche neben der spezifisch gewünschten Funktion dieser Applikation auch noch eine versteckte Schadsoftwarekomponente beinhalten. Diese Malware wird auch als trojanisches Pferd bezeichnet und oft zum Ausspähen von Passwörtern oder auch zur illegalen Benutzung der Ressourcen durch Dritte verwendet. Trojaner sind oft schädlicher Beipack zu kostenlosen Programmen und Tools im Internet (Kaspersky, 2008, S. 63).

2.7.4 Backdoor

Backdoor ist eine weitere Schadsoftware, welche durch vorgenannte Malware eingebracht werden kann und ermöglicht Dritten, Ressourcen des kompromittierten Computersystems zu benutzen. Die Systeme können zum Bespiel als Spamverteiler verwendet oder auch für Denial of Service-Attacken missbraucht werden (Kaspersky, 2008, S. 63).

2.7.5 Spyware

Spyware sammelt unbemerkt persönliche Daten des Benutzers/ der Benutzerin. Diese Daten können Login-Informationen und Passwörter der BenutzerInnen beinhalten oder auch Daten über das Nutzerverhalten im Internet für Werbezwecke für unberechtigte Dritte sammeln. Die Systeme werden normalerweise bei dieser Malware nicht in ihrer Funktion gestört (Kaspersky, 2008, S. 75).

2.7.6 Adware

Adware (Advertising/ Reklame und Software) benennt Computerprogramme, die Werbeanzeigen als Bestandteil der Software aufweisen. Üblicherweise handelt es sich bei Adware um zeitlich noch funktionell eingeschränkte, kostenlose Versionen. Durch die Werbeeinnahmen kann die Applikation kostenlos zur Verfügung gestellt werden. Oft existieren neben dieser Variante auch lizenzpflichtige Vollversionen ohne Werbung (Kaspersky, 2008, S. 73).

In folgender Tabelle wird die zeitliche Zunahme der Malware-Signaturen gezeigt:

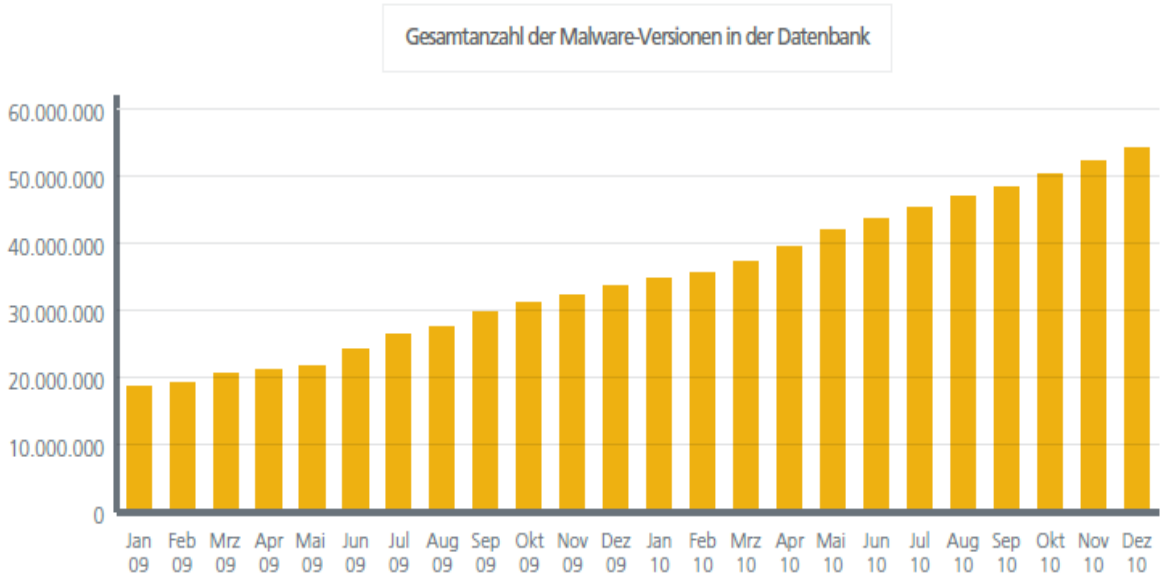

Abbildung 5: Anzahl Malware-Signaturen, Quelle (McAfee Threat-Report 4Q2010, 2011)

2.8 **Gefahren aus dem Internet**

Schaltet man einen Rechner an das Internet, dann kann dies bekanntermaßen sehr gefährlich sein. Hauptgrund dafür ist, dass die meisten Internetverbindungen TCP-Verbindungen sind, welche zwingend verlangen, dass ein Datenaustausch sowohl vom Client zum Server als auch vom Server zum Client, also bidirektional, stattfindet. Es ist (im Regelfall) nicht sinnvoll und möglich, einen Rechner einseitig an das Internet zu bringen und sicherheitshalber Daten nur zu senden, aber nichts zu empfangen. Einerseits möchte man als Internetanwender natürlich Daten wie Web-Seiten oder E-Mails empfangen. Andererseits verlangt das TCP-Protokoll, dass zumindest die Bestätigungspakete des TCP-Layers an den Client zurück, d.h. in das zu schützende Netz hinein, übertragen werden, selbst wenn nur eine E-Mail versendet wird. So ist es zwangsweise erforderlich, einen Zugang für Pakete aus dem Internet in das eigene Netz zu gestatten. Dieser ist im einfachsten Fall unkontrolliert, wird aber heute fast immer durch Firewalls in geregelte Bahnen gebracht. Das Anschalten eines Rechners an das Internet ohne Firewall ist mittlerweile nicht mehr statthaft, schon nach wenigen Minuten sind die ersten Angriffe zu erwarten, die vor allem Windows-PCs nachhaltig schädigen.

Grundsätzlich ist mit den folgenden verschiedenartigen Gefahrenquellen aus dem Internet zu rechnen:

Einerseits ist es - aus oben erwähnten Gründen - immer möglich, aus dem Internet heraus auf einen anderen im Internet befindlichen, ungeschützten Rechner missbräuchlich zuzugreifen, andererseits ist es potenziell möglich, dass Daten auf dem Weg durch das Internet abgehört und möglicherweise auch verändert werden. Weiters ist es mittlerweile weit verbreitet, fremden Personen Informationen mit schädigendem Inhalt zu senden, z.B. zerstörerische Programme oder solche, die die Ressourcen und Identität des Opfers missbrauchen. Es ist auch nicht auszuschließen, dass jemand eine falsche Identität, z.B. in Form einer falschen IP-Adresse, vorgibt (spoofing), denn die Authentizität des Absenders kann normalerweise nicht garantiert werden. Eine beliebte Attacke ist auch, einen normalen Zugriff auf einen Server nur vorzutäuschen, dies aber so oft, bis die Ressourcen des Servers erschöpft sind (Denial of Service). Gegen die bisher genannten Gefahren kann der Netzwerktechniker ankämpfen, ohne Details der Applikation zu kennen. Immer häufiger tauchen aber Probleme mit den für den Betrieb von Internetdiensten erforderlichen Serverprogrammen auf. Diese können z.B. durch besondere Eingabedaten in einen fehlerhaften Zustand versetzt werden. Verbreitet ist das Provozieren eines stack overflow, der dem Angreifer den uneingeschränkten Zugriff auf den Server und sein umgebendes Netz erlaubt (Russel, 2004).

2.9 **Social Engineering**

Unter einem Vorwand auf ihre Kennwörter hin gefragt, geben die meisten AnwenderInnen diese auch an fremde Personen weiter. Computer- und Netzwerksicherheit kann man also nur so erlangen, wenn auch den AnwenderInnen die Problematik bewusst ist und sie im Umgang mit sicherheitsrelevanten Informationen geschult werden. Insbesondere ist darauf zu achten, dass keine rückwärtigen Löcher ins Netz hinter einer Firewall gebaut werden, z.B. durch Modems an Geräten, die potenziell routen können oder ungesicherte WLAN-Access-Points. Es ist anzustreben, dass in einem Netz nur ein einziger Sicherheitsgateway zum Internet hin aufgebaut wird, über das sämtliche Kommunikationsbeziehungen laufen, um den Überblick bewahren zu können. Dieser muss allerdings sorgfältig gewartet und beobachtet werden. Ein beliebter Angriffspunkt ist auch die Putzfrau oder anderes Personal, das gebeten wird, Datensicherungsbänder zu entwenden o.ä. Da mittlerweile die Netzwerke dank modernster Firewall-Technologie fast nicht mehr angreifbar sind, ist man dazu übergegangen, den AnwenderInnen kritische Informationen durch bewusstes Irreführen direkt zu entlocken (Phising). Auch hier hilft nur das Training der AnwenderInnen, um derartige Absichten zu erkennen (Lipski, 2009).

3 Technische Maßnahmen, um potenziellen Gefahren entgegenzuwirken

Es geht also darum,

- Daten zu schützen, die auf Rechnern im Internet liegen (ruhende Daten) und Systeme mit Internetverbindung im Allgemeinen.
- Daten zu schützen, solange sie im Internet unterwegs sind (bewegte Daten).
- Daten zu untersuchen, die man empfängt, weil sie schädigenden Inhalt haben könnten, wie z.B. Computerviren.
- die Identität des Kommunikationspartners zu überprüfen.

Abhilfe schafft man, indem Rechner, die an das Internet angeschlossen werden,

- unter den Schutz einer Firewall gestellt werden oder selbst jeden Zugriff überprüfen
- Daten auf dem Weg durch das Internet verschlüsseln und digital signieren
- mit geeigneten Datenscannern ausgestattet werden, um gegen Dateien mit schädlichem Inhalt (malicious content) vorzugehen
- Absender von Daten - mit Methoden der Kryptographie und durch Vergleich von Zertifikaten - authentifizieren, möglichst auf verschiedenen Netzwerkebenen (Verschlüsselung von IP-Paketen und Verschlüsselung von E-Mails).

Immer öfter trifft man auch auf Intrusion-Detection-Systeme (IDS) oder Intrusion-Prevention-Systeme (IPS), welche wie ein Virenscanner den Netzwerkverkehr auf Anomalien hin untersuchen, Angriffe protokollieren und einen erkannten Angreifer aktiv aussperren.

3.1 **Firewall**

Zur Minimierung der Sicherheitsrisiken im Internet stellt man einzelne Rechner (host based firewall) oder auch ganze Netze (network based firewall) unter den Schutz einer Firewall.

Ein Firewallsystem besteht aus einer Firewall, welche um zusätzliche Sicherheitseinrichtungen wie einen Virenscanner, Verschlüsselungseinrichtungen usw. erweitert wurde. Die Firewall selbst stellt den Kern eines Firewallsystemes dar.

Ablauf der wichtigsten Internetdienste

Im Internet kommt durchwegs das Client-/ Server-Prinzip zur Anwendung. Ein Rechner, der eine Verbindung wünscht (der Client), sendet eine Verbindungsanforderung an den Anbieter eines Netzwerkdienstes (den Server). Je nach Wesen des Dienstes kommt eine einzige TCP- oder UDP-Verbindung zustande oder auch mehrere. Im häufigsten Fall ist es eine einzige TCP-Verbindung, die der Client Richtung Server aufbaut. Voraussetzung für einen erfolgreichen Verbindungsaufbau ist eine Erreichbarkeit auf Layer 3, die manchmal durch einen ping-Befehl überprüft werden kann. Zu Beginn fordert der Client mit seiner Absender-IP-Adresse (source address) unter einem Absenderport (source port) eine Verbindung an einer Ziel-IP-Adresse (destination address) an einem Empfängerport (destination port) an. Die Empfängerportnummer zeigt in der Regel an, welcher Dienst gewünscht wird. Für die Zuordnung der Port-Dienste gibt es vor allem für den Bereich bis Port 1024 Vorgaben (well known ports), die aber nicht zwingend sind. Durch ein Telnet an die Empfängeradresse und den Empfängerport kann jede beliebige Verbindung simuliert werden (z.B. Telnet an www.firma.at, port 80, es meldet sich der Web-Server, man kann dann ein http-Kommando eingeben) (Deal, 2005).

Bei standardgemäßer Einstellung laufen die wichtigsten Internetdienste folgendermaßen ab:

telnet tcp,	Client verbindet mit Absenderport > 1023 auf port 23 am Server
ssh tcp,	Client verbindet mit Absenderport > 1023 auf port 22 am Server
http tcp,	Client verbindet mit Absenderport > 1023 auf port 80 am Server
https tcp,	Client verbindet mit Absenderport > 1023 auf port 443 am Server
ftp tcp,	Client verbindet mit Absenderport > 1023 auf port 21 für die Steuerungsverbindung, dann verbindet der Server in einer zusätzlichen Datenverbindung von Port 20 oder einem port > 1023 auf einen vereinbarten port > 1023 am Client
ftp passiv tcp,	Client verbindet mit Absenderport > 1023 auf port 21 für die Steuerungsverbindung, dann verbindet der Client von einem port > 1023 auf port 20 oder einen port > 1023 am Server für die Datenverbindung
news tcp,	Client verbindet mit Absenderport > 1023 auf port 119 am Server
smtp tcp,	Mailsender verbindet mit Absenderport > 1023 auf port 25 am SMTP-Mailempfängerserver
pop tcp,	Client verbindet mit Absenderport > 1023 auf port 110 am Server
imap tcp,	Client verbindet mit Absenderport > 1023 auf port 143 am Server
DNS	Einfache Anfragen erfolgen über UDP vom Client mit Absenderport > 1023 auf port 53 des DNS-Servers. Ganze Zonentransfers erfolgen über TCP vom Client mit Absenderport > 1023 auf port 53 des DNS-Servers.

Die Firewall hat folgende beiden Grundaufgaben zur Absicherung des Internetzuganges zu bewerkstelligen:

- Erlauben und Sperren bestimmter Pakete und Verbindungen aufgrund von Informationen von Layer 3 und Layer 4, eventuell auch darüber liegender Layer (Paketfilter)
- Verbergen der internen Netzwerkadressen und Netzwerkstruktur (NAT, Proxy und Applikation-Gateway)

3.1.1 Firewall-Paketfilter

Paketfilter bedienen sich der Daten von Layer 3 und 4, moderne Paketfilter auch der Layer 5 bis 7. Aus Layer 3 und 4 lässt sich analysieren:

- Layer-4-Protokolltyp (TCP, UDP, ICMP, ...)
- Absender-IP-Adresse
- Empfänger-IP-Adresse
- Absender-Portnummer
- Empfänger-Portnummer
- Richtung des Verbindungsaufbaues
- Informationen aus diversen Flags

Aufgrund dieser Informationen kann im Einzelfall vom Paketfilter entschieden werden, ob ein Paket oder eine Verbindung akzeptiert oder abgewiesen wird.

Damit ist man in der Lage, nach dem Anschluss eines Rechners oder eines Netzes an das Internet festzulegen, welcher Rechner mit welchem anderen Rechner mit welchen Diensten betrieben werden darf. Dabei kann unterschieden werden, ob die Verbindung abgehend oder ankommend ist.

Paketfilter können für ein ganzes Netzwerk implementiert werden oder auch nur für einen einzigen Rechner, was in letzter Zeit neben den Netzwerkfirewalls zum internen Schutz im Intranet immer mehr Verbreitung bekommt.
Das Abweisen von Verbindungen kann auf zweierlei Arten erfolgen. Entweder erhält der Eindringling eine Antwort, dass er den gewünschten Dienst nicht benutzen darf, was immerhin verrät, ob es diesen Rechner oder Dienst gibt (reject mode), oder die Pakete des Verbindungsaufbaues werden kommentarlos verworfen, wobei der Eindringling keinerlei Information hat, ob der attackierte Service überhaupt existiert (drop mode). Seine Anwendung wird in einen Time-out laufen (Deal, 2005, S. 47).

Stafeful Filtering

Dynamische Paketfilter (stateful filtering) sind eine Weiterentwicklung der Paketfilter, die eine wesentliche Erhöhung der Sicherheit bringen. Hierbei verwaltet der Paketfilter den Status einer TCP-Verbindung und eventuell auch einen virtuellen Status einer UDP- oder ICMP-Verbindung (Internet-Control-Message-Protocol). Einfachere Versionen beachten dabei die diversen Flags von TCP noch nicht im vollen Umfang. Während bei statischen Paketfiltern eine Regel einzubauen ist, dass Antworten auf TCP-Anfragen aus dem Internet permanent erlaubt sind, gibt ein dynamischer Paketfilter diesen Weg erst nach einer entsprechenden Anfrage frei. Er bleibt auch nur offen, bis mit Finish-Flag (FIN) oder Reset-Flag (RST) die Sitzung beendet wurde, oder verfällt nach einer einstellbaren Zeit. Während also bei statischen Paketfiltern der Rückweg ins interne Netz permanent offen sein muss, öffnet man bei dynamischer Filterung diesen nur nach einer Anfrage, und dann auch nur für diese eine Anfrage (Deal, 2005, S. 53).

Stateful Inspection

Bei stateful inspection, oft auch SPI (stateful packet inspection) genannt, beschreibt man nur die ersten Pakete eines Verbindungsaufbaues als erlaubt, die Regeln für Folgepakete findet der Filter selbst. Dazu muss er Protokollinformationen höherer Schichten verarbeiten können, weil z.B. bei ftp und H.323 innerhalb einer Steuerverbindung die Parameter weiterer dynamisch auf- und abzubauender Verbindungen ausgehandelt werden. Bei Paketfiltern mit stateful inspection ist daher zu überprüfen, welche Anwendungen sie kennen. Einfache TCP-Dienste mit einem einzigen Port-Paar (wie z.B. telnet, ssh, http, SMTP) sind aber in jedem Fall unterstützt (Deal, 2005, S. 53).

Deep Packet Inspection

Deep Packet Inspection kurz DPI stellt den nächsten Schritt in der Entwicklung dar und dient zur Überwachung der zu übertragenden Datenpakete. Dabei werden der Headerteil und der Datenteil auf Protokollverletzungen, Malware, Spam und sonstige Anomalien untersucht.
Durch diese Technologie kann der Datentransfer in den verschiedenen OSI-Schichten abgesichert werden (Deal, 2005, S. 54).

3.1.2 Firewall - Adressen verbergen

Die Adressierung der Datenpakete und das Routing im Internet sind zunächst immer Ende zu Ende-Beziehung. Dies bedeutet, dass der Absenderrechner seine IP-Adresse in das IP-Paket zu schreiben hat und als Empfängeradresse die IP-Adresse des anderen Endsystems, nicht etwa die IP-Adresse eines Routers. Da Source-Routing im Allgemeinen nicht verwendet wird, hat jeder Router in der Laufbahn des Paketes einzig aufgrund der Ziel-IP-Adresse zu entscheiden, wohin das Paket weiterzuleiten ist.

Solcherart exportiert man mit jedem IP-Paket seine eigene IP-Adresse, und am Internetanschluss sind alle internen IP-Adressen eines Unternehmens zu finden, womit auch die interne Netzstruktur offenbart wird.
Die Sicherheit eines Internetzuganges erhöht sich ganz erheblich, wenn der Angreifer die Adressen der internen Rechner und damit auch die Struktur des internen Netzwerkes nicht kennt. Man hat deshalb den Wunsch, diese zu verstecken. Noch besser ist es, wenn darüber hinaus intern noch Adressen verwendet werden, die im Internet ungültig sind. Der Einsatz dieser Verfahren wurde auch durch die drohende Adressknappheit im Internet massiv vorangetrieben, weil damit offizielle Internetadressen eingespart werden können. Im Normalfall erhält man zu einem Internetanschluss 6 oder 14 offiziell gültige IP-Adressen, was für die Adressierung aller Rechner in einem internen Netz in vielen Fällen nicht ausreichend ist. Sie erhalten deshalb interne Adressen, die in offizielle umgewandelt werden, wenn sie ein Datenpaket in das Internet versenden.

Es sind hierfür zwei Verfahren verbreitet. Einerseits Network-Address-Translation (NAT) oder andererseits Proxies (Stellvertreter) und Applikation-Gateways (Deal, 2005, S. 72)**.**

Der Requests for Comments (RFC) 1631 aus dem Jahre 1994 definiert ein Verfahren, wie Firmen ihre internen Adressen beim Zugriff auf das Internet verstecken können. Die Intention war zuerst die Weiterverwendbarkeit inoffizieller Adressen, weil sehr oft an den Rechnern IP-Adressen eingestellt waren, die jemand anderem gehörten.

Private IP-Adressen

Im Grunde können nun intern beliebige Adressen vergeben werden, weil sie im Internet nicht aufscheinen. Würde allerdings in diesem Beispiel intern ebenfalls das Netz 193.80.12.0 (keine private IP-Adresse) verwendet, dann wäre ein korrektes Routing des Paketes nicht möglich, weil der Web-Server von den PCs im internen Netz per ARP-Request gesucht würde. Es ist also sicherzustellen, dass intern Adressen eingestellt werden, die im Internet nicht vorkommen. Dafür wurden in RFC 1597 die so genannten privaten Adressen festgelegt (Wikipedia, 2011).

Netznummern privater IP-Adressen

- Class A: 10.
- Class B: 172.16. bis 172.31
- Class C: 192.168.0 bis 192.168.254

Diese Adressen werden niemals die offiziellen IP-Adressen eines Netzes im Internet sein. So ist eine Verwechselungsgefahr ausgeschlossen.

Application-Gateways

Einen anderen Ansatz zum Verstecken interner Netzstrukturen stellen die Application-Gateways (AGW) dar. Der gravierende Unterschied zwischen NAT und AGW besteht darin, dass im Falle von NAT wie gewohnt eine TCP-Session vom Client zum Ziel-Server aufgebaut wird, während beim AGW eine TCP-Session vom Client zum AGW aufgebaut wird, und eine weitere vom AGW zum Ziel-Server, also insgesamt zwei Sessions (Stein, 2008, S. 402).
Vorteile von AGWs:

- Hohe Sicherheit, weil es die Anwendung kennt
- Kann anwenderbezogen arbeiten und Dokumente zwischenspeichern oder sogar auf Viren scannen

Nachteile von AGWs:

- Sehr aufwändig, meist ein vollwertiges Rechnersystem zusätzlich notwendig
- Nur für interaktive Dienste möglich
- Für den Anwender nicht transparent, Anwender müssen instruiert werden, wie mit dem AGW umzugehen ist

Proxies - Stellvertreter

Um die Firewall für den Anwender transparent zu machen, installiert man statt der AGWs auch Proxies, z.B. einen Web-Proxy. Proxies arbeiten in derselben Weise wie AGWs, allerdings bedient nicht der Anwender das AGW, sondern die Applikation ohne sein Zutun von sich aus. Damit sind Proxies für den Anwender transparent. Allerdings muss die Applikation an den Proxy angepasst und damit verändert werden. Sie muss wissen, wie man den Proxy bedient. Die bekannteste Applikation mit Proxy sind die Web-Browser. Diese greifen selten auf die Web-Server im Internet selbst zu, sondern nur auf einen einzustellenden Proxy, der dann stellvertretend für den Client das angeforderte Dokument aus dem Internet holt. Es gibt also auch wieder zwei TCP-Sessions für einen Web-Zugriff. Deshalb wird im Internet nur die Adresse des Proxies bekannt, während jene des Clients verborgen bleibt. Der Web-Proxy kann auch mit einem Cache (Zwischenspeicher) versehen werden, und das angeforderte Dokument statt vom Originalserver direkt aus seinem Speicher holen, sofern es dort in einer aktuellen Version hinterlegt ist. Das erspart Übertragungsvolumen. Für jede gewünschte Applikation ist ein geeigneter Proxy zu installieren, weil dieser das Applikationsprotokoll im Detail verstehen muss (Stein, 2008, S. 403).

Socks

Der Socks-Server ist ein generischer Proxy. Normale Proxies sind für ein bestimmtes Protokoll gebaut (z.B. http-proxy, ftp-proxy). Der Socks-Server agiert wie ein Proxy, allerdings teilt der Client dem Socks-Server bei jeder Verbindung vorab mit, welchen Dienst er wünscht. Auf diese Weise kann der Socks-Server für beliebige Verbindungen eingesetzt werden. Allerdings muss die Applikation so umgestellt (socksified) werden, dass sie statt einer direkten Verbindung ins Internet automatisch den Weg über den Socks-Server wählt. Dies ist der Nachteil des Socks-Verfahrens, dafür ist es aber für den Anwender transparent (Stein, 2008, S. 403).

Port-Translation und Plug-Gateway

Hierbei definiert man einen oder mehrere Ports an der Firewall als „virtuelle Server“. Sobald auf diesen Port verbunden wird, stellt die Firewall eine weitere Verbindung zu einer vordefinierten Adresse an einem vordefinierten Port her. Der News-Zugriff erfolgt z.B. meist so, dass man den NNTP-Port 119 an der Firewall von innen fix mit Port 119 am News-Server des Providers verbindet. Greift man auf Port 119 an der Firewall zu, dann stellt dieser umgehend eine weitere Verbindung mit dem wahren News-Server her und holt den gesuchten Artikel. Es bestehen dann zwei TCP-Verbindungen, eine zwischen dem Client und dem Plug-GW, die zweite zwischen dem Plug-GW und dem News-Server. So wird nur die Adresse des Plug-GW im Internet sichtbar. Als News-Server ist an den Clients in diesem Fall die Firewall einzustellen. Natürlich kann das Plug-GW auch in der entgegengesetzten Richtung für Zugriffe aus dem Internet in das interne Netz verwendet werden. Bei kleinen Firewalls für den Home-User findet man etwas Ähnliches, allerdings auf der Basis von NAT. Man kann festlegen, dass ein Telnet auf Port 23 der Firewall aus dem Internet an den Port 23 eines bestimmten Rechners im internen Netz weitergeleitet wird, eine Verbindung auf Port 25 (SMTP) an der Firewall an den internen Mail-Server usw. Jeder Port einer offiziellen IP-Adresse einer solchen Firewall kann genau einmal einer internen Adresse zugeordnet werden. Dies wird meist Port-Address-Translation (PAT) oder Port-Forwarding genannt.

3.1.3 Protokollierung

Das Firewallsystem sollte Angriffen natürlich von sich aus widerstehen. Dennoch ist dringend anzuraten, dass es laufend beobachtet wird, um Attacken zu erkennen. Zu diesem Zweck lässt man die Firewall-Protokolle mit variabler Ausführlichkeit anlegen, je nach Gefährdungspotenzial. In großen Netzen fällt dabei sehr viel Information an, die viel Speicherplatz braucht und auch aufwändig auszuwerten ist. Für die Protokollierung verwendet man entweder die mitgelieferten Systeme der Softwarepakete oder häufig auch den Syslog-Mechanismus von Unix. Hierbei senden die Netzwerkkomponenten ihre Nachrichten an einen zentralen Server, eine Management-Konsole im einen Fall, einen Syslog-Server im anderen (Deal, 2005, S. 109).

3.1.4 Sicherheitstests

Jedes Firewallsystem sollte regelmäßig einer Selbstevaluierung unterzogen werden. Auch hierzu gibt es entsprechende Software. Als ein Beispiel kann der Internet-Scanner gelten. Mit diesem Programm kann man sowohl seine eigene Firewall als auch andere Systeme attackieren, die Methoden dazu kommen aus einer Datenbank, die stets nach neuesten Erkenntnissen aktualisiert wird. Man erhält einen Bericht über potentielle Verwundbarkeiten nach dem aktuellen Stand der Erkenntnisse. Da ständig neue Angriffe auf Internetsysteme entwickelt und Fehler in Protokollimplementierungen gefunden werden, sind überdies laufend Softwareaktualisierungen zur Fehlerbeseitigung notwendig. Informationen darüber erhält man in einschlägigen Quellen (z.B. www.securityfocus.com).

3.1.5 Redundanz und load-sharing

Man erhält Schutz vor dem Ausfall einer Firewall durch Aufbau zweier paralleler Systeme, die entweder im hot-standby-Betrieb oder auch im load-sharing-Betrieb arbeiten können. Eine geeignete Software (z.B. stonebeat, heartbeat) sorgt dafür, dass eines der beiden Systeme die Arbeit übernimmt bzw. die Last auf beide Systeme aufgeteilt wird, solange beide intakt sind. Fällt ein System aus, dann übernimmt das wartende System die Last bzw. eines der beiden laufenden Systeme die gesamte Last. Beide Firewalls haben mindestens zwei Netzwerkinterfaces, eines ins interne Netz und eines ins Internet, und arbeiten als Router. Stand der Technik ist, dass über eine zusätzliche serielle oder LAN-Verbindung (heartbeat) die beiden Systeme den Status aller Netzwerkverbindungen austauschen, sodass das Reservesystem vom fehlerhaften System alle offenen Verbindungen im Wesentlichen ohne Datenverlust (TCP wiederholt verloren gegangene Pakete automatisch) übernehmen und weiterführen kann (Deal, 2005, S. 99).

3.1.6 Bandbreitenaufteilung

Internetbandbreite ist für Unternehmen eine sehr teure Ressource, die effizient genutzt werden muss. Auch zur Garantie einer bestimmten Performance für einzelne Dienste ist die Reservierung von Bandbreite erforderlich. Z.B. dann, wenn ein Unternehmen einen eigenen Webserver hat, dessen Übertragungsleistung nicht durch einen FTP-Transfer blockiert werden soll.

3.2 Intrusion-Detection- und Prevention-Systeme

In diesem Kapitel werden der Aufbau und die Komponenten von Intrusion-Detection-Systemen (IDS) behandelt und der Unterschied zu Intrusion-Prevention-Systemen (IPS) beschrieben.
IDS-Systeme, zu Deutsch Systeme zur Einbruchserkennung, werden eingesetzt, um Angriffe auf das Netz zu erkennen. Sie wirken wie eine Kombination aus Sniffer und Virenscanner in einem bestimmten LAN-Segment, z.B. in der Demilitarized-Zone (DMZ). Das heißt, sie analysieren den gesamten Netzwerkverkehr in einem Segment und vergleichen ihn mit Signaturen bekannter Angriffe, um diese zu erkennen. Werden verdächtige Pakete aufgegriffen, dann erfolgt durch das IDS eine Mitteilung. Darüber hinaus kann ein IPS sofort Abwehrmaßnahmen ergreifen, z.B. die Firewall-Regeln ändern, um den Angreifer explizit auszusperren. Wird IPS in der Firewall selbst implementiert, dann spricht man von Deep-Packet-Inspection. Die Signaturen werden ähnlich wie bei Virenscannern permanent aktualisiert, um neue Attacken berücksichtigen zu können (ConSecur GmbH, 2002).

3.2.1 Intrusion-Detection-System (IDS)

Der Begriff Intrusion Detection bezeichnet die Überwachung von IT-Systemen und Datennetzen mit dem Ziel der Erkennung von sicherheitstechnischen Ereignissen im Überwachungsbereich, welche auf Angriffe, Missbrauchsversuche und Sicherheitsverletzungen hindeuten. Diese Ereignisse sollen dabei zeitnah erkannt und gemeldet werden. Intrusion Detection ist als gesamter Prozess zu verstehen und es ist daher ein organisatorischer und technischer Prozess für diese Aufgabe zu definieren.

Als Intrusion-Detection-System (IDS) wird eine Kombination von Systemen bezeichnet, die den gesamten Intrusion-Detection-Prozess von der Erkennung über die Auswertung bis hin zur Eskalation und Dokumentation von Vorfällen unterstützen. Intrusion-Detection-Produkte weisen diese integrierte Funktionalität auf oder können jedoch auch aus Einzelkomponenten zusammengesetzt werden. Die Auswahl und die Zusammenstellung der Komponenten richten sich nach dem Einsatzgebiet und den organisatorischen Rahmenbedingungen (ConSecur GmbH, 2002).

Taxonomie

Intrusion-Detection-Systeme können aufgrund unterschiedlicher Parameter in bestimmte hierarchische Kategorien, auch als Taxonomie bezeichnet, eingeteilt werden. Die Kategorisierung kann anhand der Platzierung der Sensoren und Art der Erkennungsmethode von Angriffen durchgeführt werden (ConSecur GmbH, 2002).

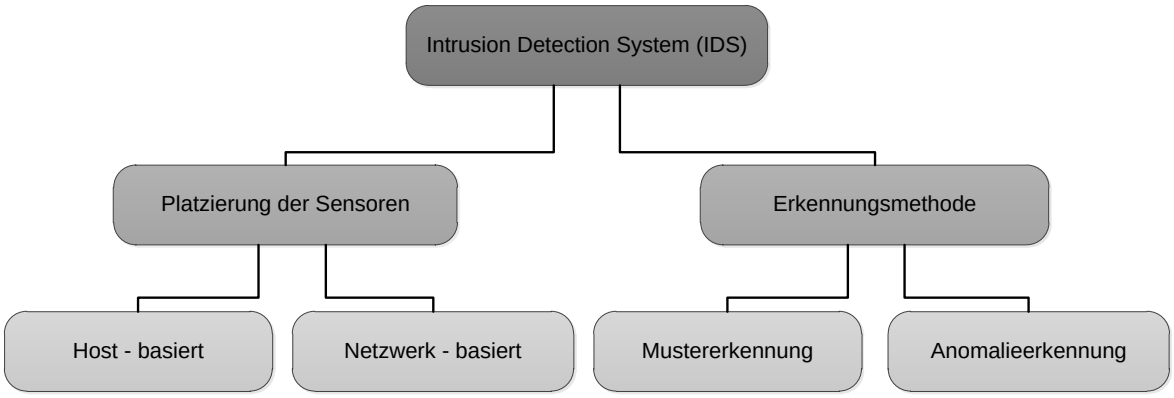

Abbildung 6: IDS-Systeme-Klassifizierung

Komponenten und Architektur

Ein Intrusion-Detection-System (IDS) besteht typischerweise aus mehreren Komponenten, welche mehrfach und optional zum Einsatz kommen:

- Netz-basierte Sensoren
- Host-basierte Sensoren
- Datenbankkomponenten
- Auswertestationen
- Managementstationen

Die Daten, welche von den Sensoren erfasst werden, erzeugen bei Angriffserkennung Ereignisdaten, welche zur weiteren Verarbeitung in einer Datei oder Datenbank gespeichert werden. Die in den Daten gespeicherten Ereignismeldungen können anschließend in einer Auswertestation analysiert und nach dem Gefährdungspotential eingestuft werden. Eine Sortierung und Klassifikation der Ereignisse wird von der Auswertestation durchgeführt. Weiters ist die Auswertestation für das Reporting der Vorfälle und auch für die Alarmierung zuständig. Die Wartung und Konfiguration erfolgt über eine Managementstation. Dies umfasst die Konfiguration und Adaption der Sensoren, Erstellung und Anpassung der Überwachungsregeln und deren Überwachungsbereiche.

Die Sensoren werden in Netz-basierte (Überwachung des IT-Datennetzes) und Host – basierte Sensoren (Überwachung des einzelnen Hosts und deren Betriebssysteme) eingeteilt (ConSecur GmbH, 2002).

Netz-basierte Sensoren

Netz-basierte Sensoren (auch Netzsensoren genannt) überwachen den Netzwerkverkehr eines einzelnen Rechners oder eines ganzes Teilnetzes auf verdächtige Ereignisse. Der Datenverkehr wird mit Hilfe eines Paket-Sniffers auf einem Netzwerkinterface mitgelesen und anschließend nach speziellen Kriterien ausgewertet. Typischerweise werden Netz-basierte Sensoren als eigene IT-Systeme ausgeführt, da diese Systeme eine hohe Rechenleistung aufweisen müssen und die zu überwachenden Systeme in ihrer Leistungsfähigkeit nicht eingeschränkt werden sollen. Sehr viele Hersteller bieten eine Kombination aus Hard- und Software, eine sogenannte Appliance, für diesen Anwendungsfall an. Netz-basierte Sensoren eignen sich sehr gut für die Erkennung von netzbasierten Angriffen, welche sich gegen mehrere Zielsysteme richten. In diesem Zusammenhang wären die Gefährdungen durch z.B. Denial-of-Service (DoS)-Angriffe zu nennen. Netzsensoren können in verschlüsselten Datenströmen leider keine sicherheitsrelevanten Ereignisse feststellen (ConSecur GmbH, 2002).

Host-basierte Sensoren

Host-basierte Sensoren (Hostsensoren) werden zur Überwachung des Betriebssystems und zur Überwachung der Applikationen auf den Hosts eingesetzt. Diese Sensoren werden direkt am Host installiert und können daher analog zum Virenschutz die Funktionsfähigkeit und die Leistungsfähigkeit des Hosts beeinträchtigen. Diese Sensoren können die Host-Systeme sehr gut überwachen und sicherheitsrelevante Ereignisse sofort entdecken und die Sicherstellung der Datenintegrität gewährleisten. Durch applikationsüberwachende Sensoren ist eine Überwachung der Applikation möglich, da weder host- noch netzwerk-basierte Sensoren die Applikation und deren Prozesse überwachen können.

Datenbankkomponenten

Intrusion-Detection-Systeme erzeugen bei der Angriffserkennung Ereignisdateien, welche zur späteren Verarbeitung gespeichert werden müssen. Je nach Datenmenge und Aufbewahrungszeitraum werden diese Daten in Dateien oder in den verschiedensten Datenbankformen abgelegt. Standardmäßig werden Datenbanken mit bekannten Schnittstellen mit SQL-Technik bevorzugt.

Managementkomponenten

Mittels der Managementstation erfolgen die Konfiguration und die Kalibrierung eines Intrusion-Detection-Systems. Dies umfasst folgende Funktionalitäten (ConSecur GmbH, 2002):

- Konfiguration der IDS-Komponenten
  (Sensoren, Datenbanken, Managementstationen)
- Einstellen der Kommunikationsparameter der IDS-Komponenten untereinander (IP-Adressen, Namensgebung, Kryptoschlüssel, Lebenszeichen-Intervall)
- Aufnahme der zu überwachenden Objekte (Netze, IT-Systeme, Hosts)
- Erstellung und Anpassung von Überwachungsregeln und Erstellung von "IDS-Policies"
- Gruppierung von IDS-Sensoren
- Zuweisung der "IDS-Policies" zu Sensoren oder Sensorengruppen

Auswertungsstation

Die Auswertungsstation wird für das Reporting und zur Analyse der aufgezeichneten Systeme verwendet.

- Kommandozeilen-Interface
- Webbasierte Schnittstelle
- IDS-eigene Auswertungsoberfläche
- Anzeige eingehender Meldungen
- Sortierung der Ereignisse
- Klassifikation der Ereignisse
- Reaktion und Alarmierung
- Ablage der Ereignisdaten zur späteren Weiterverarbeitung
- Reporting-Funktionen können sowohl zur Generierung von Managementreports und -statistiken als auch zur Langfristanalyse der Meldungen eingesetzt werden

3.2.2 Methoden der Angriffserkennung

Bei fast allen Anbietern werden diese drei bekannten Verfahren zur Erkennung von Angriffen verwendet

- Erkennung von Angriffsmustern
- Anomalie-Erkennung
- Korrelation von Ereignisdaten

Erkennung von Angriffsmustern

Angriffe werden bei Signatur-basierten Intrusion-Detection-Systemen (IDS) durch den Vergleich (Pattern Matching) des Netzwerkverkehrs mit bekannten Angriffsmustern erkannt. In diesem Zusammenhang werden die Muster des Angriffes als Signaturen bezeichnet. Diese Signaturen können einfache Zeichenketten oder komplexe Angriffsmuster enthalten. Wird eine bekannte Signatur im Netzwerkverkehr von der IDS erkannt, so wird umgehend ein Alarm ausgelöst und das entsprechende Datenpaket gespeichert. Um einen Angriff zu erkennen, muss die Signatur in sämtlichen Modifikationen vorhanden sein, um einen Alarm auszulösen zu können. Die Signaturerkennung kann auch auf den normalen Datenverkehr zutreffen und daher auch Fehlalarme auslösen.

Anomalieerkennung

Die Erkennung von Angriffen in Form von Anomalien erfolgt durch Abweichungen zum normalen Netzwerkverkehr und Abweichungen zum Normalverhalten eines IT-Systems. Es gibt verschiedene Verfahren, um Anomalien zu erkennen (ConSecur GmbH, 2002):

Protokollanalyse

Bei der Protokollanalyse wird der Netzwerkverkehr auf Anomalien untersucht. Weicht das verwendete Protokoll vom definierten Protokollstandard ab, so kann eine Anomalie erkannt werden. Da viele Angriffe in IP-Netzen erfolgen, kann durch die gut spezifizierten Protokollstandards eine recht zuverlässige Art der Angriffserkennung angewandt werden.
Diese Methode verfügt über eine gute Performance, da die Signaturen und deren mögliche Modifikationen nicht abgearbeitet werden müssen. Nachteilig ist zu erwähnen, dass bei dieser Methode durch Fehler und Unschärfen im Protokoll eventuelle Angriffe von den IDS-Systemen nicht erkannt werden können und daher einige Systeme zusätzlich Signatur-basierte Methoden zur Angriffserkennung bei der Protokollanalyse verwenden.

Anomalieerkennung auf Basis statistischer Daten

Bei dieser Art der Anomalieerkennung werden statistische Kennwerte festgelegt und das Systemverhalten mit den festgelegten statistischen Werten verglichen. Das Normalverhalten eines Systems wird durch unterschiedliche Objekte (Nutzer, Dateien, Anwendungen, Services, etc.) und den dazugehörigen Verhaltensweisen (Anzahl der Anmeldungsversuche, Nutzungsdauer, Betriebszeiten, Anzahl der gleichzeitigen User, etc.) festgelegt. Anhand dieser statistischen Werte kann festgestellt werden, ob eine signifikante Verhaltensänderung zum Normalbetrieb vorhanden ist.

Anomalieerkennung auf Basis künstlicher Intelligenz

Zusätzlich werden bei dieser Art der Anomalieerkennung, auf Basis statistischer Daten, zusätzlich künstliche Intelligenz bzw. selbstlernende Systeme bei der Analyse der Angriffsmuster verwendet. Einige IDS arbeiten mit neuronalen Netzen, bei denen als Eingabeparameter System- und Netzwerkaktivitäten zugeführt werden, um nach einer Lernphase Nutzer- und Rechenprofile für die Erkennung von Anomalien zu bilden.

Anomalieerkennung auf Basis von Honeypots

Honeypots sind eigene IT-Systeme (Server, Netzwerke, Programme, Services), welche keine produktive Funktion haben und für die Angreifer als Fallen verwendet werden. Oft werden betriebskritische und sicherheitskritische Systeme den Angreifern vorgetäuscht. Ein Honeypot hat ein einfaches, vordefiniertes, statisches Betriebsverhalten und jegliche Änderung von diesem vordefinierten Betriebsverhalten kann als Anomalie eingestuft werden.

Korrelation von Ereignisdaten

Unter Berücksichtigung von mehreren Sensoren unterschiedlichster Funktionsweisen können Ereignisse durch eine spezielle Auswertelogik besser erkannt werden. Weiters ist auch eine Korrelation von Signatur-basierten und Protokoll-basierten Erkennungsmethoden möglich.

3.2.3 Intrusion-Prevention-Systeme (IPS)

Als Intrusion-Protection/Prevention-System (IPS) werden Systeme bezeichnet, welche auf erkannte Angriffe reagieren können und geeignete Gegenmaßnahmen einleiten können. Intrusion-Detection-Systeme arbeiten in ihrer Funktionsweise passiv und zeigen Sicherheitsvorfälle auf. Intrusion-Protection-Systeme können die Ausführung von Angriffen verhindern und durch automatisierte Gegenmaßnahmen können Angriffe wie folgt verhindert werden:

- Temporäre Änderung der Regeln der Firewall, um Zugriffe zu sperren
- Beenden der Kommunikationsbeziehung
- Sperrung von Zugriffrechten auf Systeme

In Zusammenarbeit mit anderen Sicherheitseinrichtungen kann die Funktionalität eines IPS-Systems wesentlich erhöht werden. Daher können folgende zusätzliche Schutzmaßnahmen eingesetzt werden:

Virtuelle Software-Patches

Durch Virtuelle Software-Patches können Sicherheitslücken in Applikationen geschützt werden.

Client-Applikationsschutz

Schützt Endanwender gegen Angriffe auf alltägliche Anwendungen wie Microsoft Office, Adobe-PDF, Multimedia-Dateien und Web-Browsern etc.

Web-Applikationsschutz

Schützt Webanwendungen vor anspruchsvollen Applikationsangriffen wie SQL-Injection, XSS (Cross-Site-Scripting), PHP-Datei-Include, CSRF (Cross-Site Request-Forgery) und weiteren Angriffen.

Erkennung von Gefährdungen und deren Verhinderung

Erkennt und verhindert ganze Klassen von Bedrohungen, welche bestimmte Schwachstelle ausnutzen können.

Datensicherheit

Überwacht und identifiziert unverschlüsselt persönlich identifizierbare Informationen (PII) und andere vertrauliche Informationen.

Applikationskontrolle

Schützt vor nicht autorisierten Anwendungen und Risiken in definierten Segmenten des Netzwerks, wie ActiveX-Fingerprinting, Peer to Peer, Instant Messaging und Tunnelbau.

3.3 **Malwareschutz**

Eines der größten Probleme der vernetzten Computerwelt sind Computerviren. Deshalb ergänzt man Firewall-Systeme häufig um einen Virenscanner, der alle Dokumente untersucht, die die Firewall per http, FTP oder SMTP passieren. Virenscanner erkennen auch Viren in (mehrfach) komprimierten Dateien (Zip-Files). Eine Erkennung versagt aber naturgemäß, wenn Viren z.B. in verschlüsselten E-Mails eingebettet sind. Bei Firewall-Packet-Filter- Systemen geschieht die Anbindung des Virenscanners über das CVP-Protokoll. Die Firewall schaltet sich in jeden Transfer ein. Sie empfängt zuerst stellvertretend die Datei, sendet sie aber erst zum Virenscanner zur Analyse bzw. Reparatur, ehe sie zum Client weitergegeben wird.

Es sollte ein Scanner eingesetzt werden, der möglichst viele Virengattungen und Viren erkennt (z.B. Active-X-Viren, Java-Viren, Dateiviren, Bootsektor-Viren, Makro-Viren, Trojaner, Backdoor, Dialer, Würmer, Hoaxes). Die Virensignaturen werden ständig aktualisiert, bei Bekanntwerden eines Virus auch auf explizite Anforderung.

3.4 **E-Mail- und SPAM-Filter**

SPAM ist unerwünschte Information, die meist per E-Mail weiterverbreitet wird. Den Internet-AnwenderInnen entsteht Schaden, weil ihre technischen Ressourcen vergeudet werden (Leitungskapazität, Speicherplatz) und die MitarbeiterInnen mit der Bearbeitung von SPAM aufgehalten werden. Zur Abwehr von SPAM setzt man technische Filtersysteme ein, die Mails aufgrund von Mail-Adressen, Empfängeranzahl, Größe, Stichworten, Headereinträgen, Art von Attachments usw. filtern. Die Filterung kann auf verschiedenen Systemen erfolgen, um eine bestmögliche Säuberung der Spams zu erreichen.

3.5 **URL-Filterung**

Der Internetzugang für MitarbeiterInnen in Unternehmen wird in der Regel gestattet, insoweit aber eingeschränkt, indem URLs mit unerwünschtem Inhalt ausgeblendet werden. Professionelle Anbieter katalogisieren bekannte Adressen in Kategorien, diese können dann abhängig vom Anwender, von der Tageszeit usw. freigegeben oder gesperrt werden.

3.6 **Authentifizierung**

Firewalls können in der Regel ihre Entscheidungen nur auf Basis der IP-Adressen in Datenpaketen treffen. Der Wunsch ist aber, nicht einzelnen Rechnern, sondern den Personen dahinter, Rechte zu erteilen. Zu diesem Zweck hat sich der Anwender/ die Anwenderin an der Firewall zu authentifizieren. Auch für die Einwahl in Netze wird meist eine Authentifizierung verlangt. Methoden der Authentifizierung sind, mit steigender Sicherheit:

- Passwörter
- Einmal-Passwörter (S/Key)
- Secure-ID
- Keycards und Security-Tokens
- Biometrische Systeme

Die Netzwerkkomponenten kommunizieren meist über die Protokolle RADIUS oder TACACS mit dem System, welches die Berechtigungen verwaltet. Aus der OSI-Welt kommend, findet auch die LDAP-Technologie steigende Verbreitung.

3.7 **Verschlüsselung**

Die Technologie virtueller privater Netze gewinnt enorm an Bedeutung. Man versteht darunter die Möglichkeit, ein öffentliches, unsicheres, dafür aber preiswertes Netz - wie das Internet - dadurch quasi privat zu nutzen, indem man alle übertragenen Daten verschlüsselt und nur einem bestimmten Personenkreis zugänglich macht. Durch die Verschlüsselung entsteht ein privater Tunnel durch das Netz. Man kann damit eine teure Standleitung durch einen sicheren Tunnel ersetzen. Wenn sich Quality of Service (QoS) im Internet durchsetzt, können künftig für derartige virtuelle Standleitungen auch Übertragungsgarantien abgegeben werden. Die standardisierte, am meisten verbreitete, Technik dafür ist Ipsec. Da Internet Protocol Security (Ipsec) sehr rechenintensiv werden kann, wenn man hochsichere Algorithmen wie Data Encryption Standard (DES) oder Advanced Encryption Standard (AES) verwendet, kann man die Verschlüsselung nur bei niedrigen Geschwindigkeiten durch die Firewall selbst oder den Router vornehmen lassen. Bei hoher Last verwendet man dafür parallel zur Firewall eigene Systeme, welche für diese Aufgabe optimiert sind.

3.8 **Netzwerkkategorisierung**

Aufgrund der möglichen Gefährdungen von PatientInnen, AnwenderInnen und Dritten beim Betrieb von medizintechnischen Anlagen und Systemen in IT-Datennetzten kam es zu einer Kategorisierung der medizinischen Netzwerke in der Europäischen Norm DIN EN 60601-1. Diese Norm klassifiziert mit nachstehender Einteilung von Netzwerken, hinsichtlich der Folgen unter Berücksichtigung der Reaktionszeit, die mögliche Störung bzw. Schädigung eines Patienten/ einer Patientin.

Es sind daher die vernetzten medizintechnischen Anlagen, wie in der folgenden Tabelle angeführt, zu kategorisieren und diese Vorgaben sind bei der Integration in das IT-Datennetzwerk zu beachten:

Folgen	Reaktionszeit	Klasse	Beispiele
Tod schwerwiegende Verletzung	Sekunde(n)	C	Infusion (closed loop), OP-Roboter-Fehlsteuerung
	Minute(n)	C	Fehlende Alarmübertragung eines intensiv-medizinischen Netzwerkes
	Stunden(n)	C/B	Falsche Therapiedaten an Dialysemaschine oder Beatmungsgerät
mittlere Verletzung	Sekunde(n)	C/B	Falsche Alarmübertragung, OP-Roboter-Fehlsteuerung
	Minute(n)	B	
	Stunden(n)	B	Bildverfälschung, Verlust eines Therapieprotokolls

Folgen	Reaktionszeit	Klasse	Beispiele
leichte Verletzung	Sekunde(n)	B	
	Minute(n)	B	Bildverlust einer Röntgenaufnahme
	Stunden(n)	B/A	
vernachlässigbare Folgen	Sekunde(n)	A	Bild
	Minute(n)	A	Verlust eines EEGs
	Stunden(n)	A	Verlust eines Langzeit-EKGs

Tabelle 1: Klassifikation eines Netzwerkes (DIN 60601-1 3rd)

3.8.1 Netzwerkklasse A

In dieser Klasse werden alle nicht zeitkritischen medizinische Geräte und Applikationen und deren administrative Prozesse betrieben. Ein kurzfristiger Ausfall oder längere Wartungsfenster stellen für diese Anforderung keine Gefahr dar. Eine Wiederholung der Untersuchung wie zum Beispiel einer EKG- oder EEG-Untersuchung stellt für den Patienten/ die Patientin keine Gefährdung dar und kann jederzeit wiederholt werden.

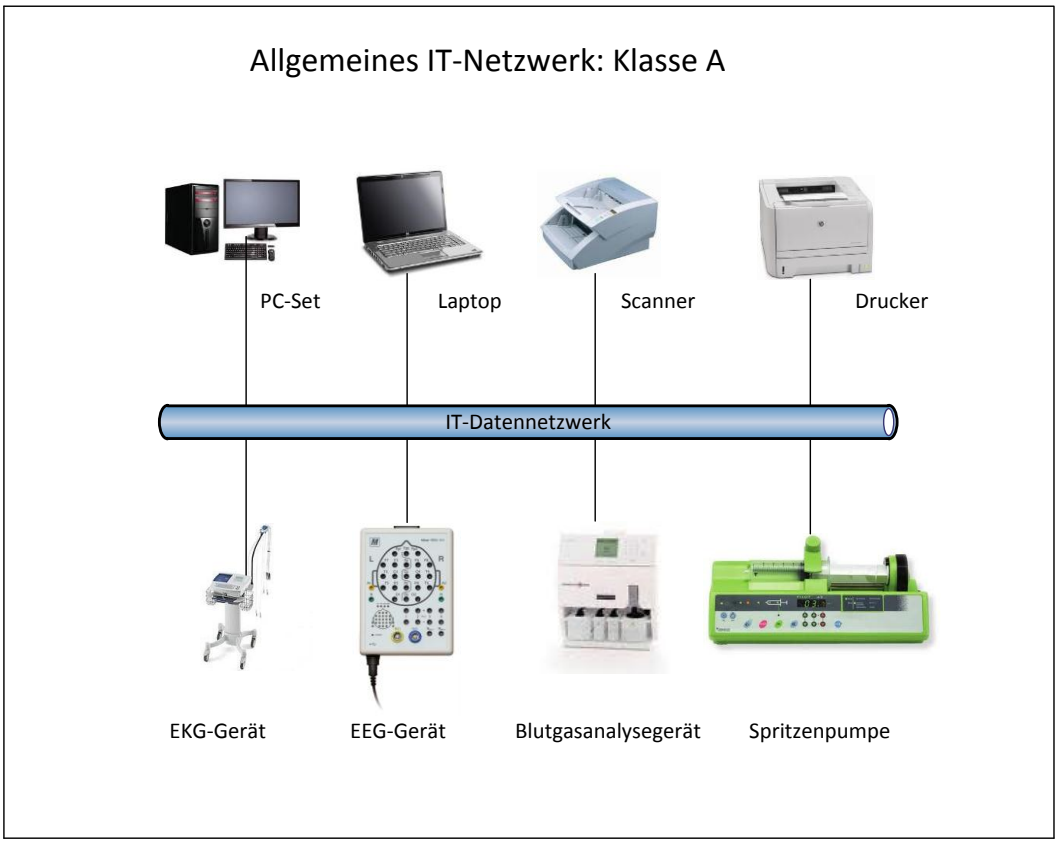

Abbildung 7: Netzwerkklasse A (DIN 60601-1 3rd)

3.8.2 Netzwerkklasse B

In dieser Klasse schlägt die Norm DIN 60601-1 3rd die Anbindung der **nichtzeitkritischen Systeme** an ein IT-Datennetz vor. Beispielhaft kann hier die Radiologie-Abteilung eines Krankenhauses genannt werden, welche eine kontrolliert gesicherte Anbindung mittels Gateway der Modalitäten benötigt.

Weiters ist eine höchstmögliche Verfügbarkeit des IT-Datennetzes sicherzustellen, da bei Ausfällen des IT-Datennetzes der laufende Betreib erheblich gestört wird. Eine Wiederholung der Röntgenuntersuchung ist bereits als kritisch zu sehen, da der Patient/ die Patientin einer zusätzlichen Strahlenbelastung ausgesetzt ist. Geräte in der Radiologie-Abteilung sind daher der IT-Datennetzwerkklasse B zuzuordnen und sollen auch mit der höchstmöglichen Verfügbarkeit des IT-Datennetzwerkes und der dazugehörigen Komponenten betrieben werden.

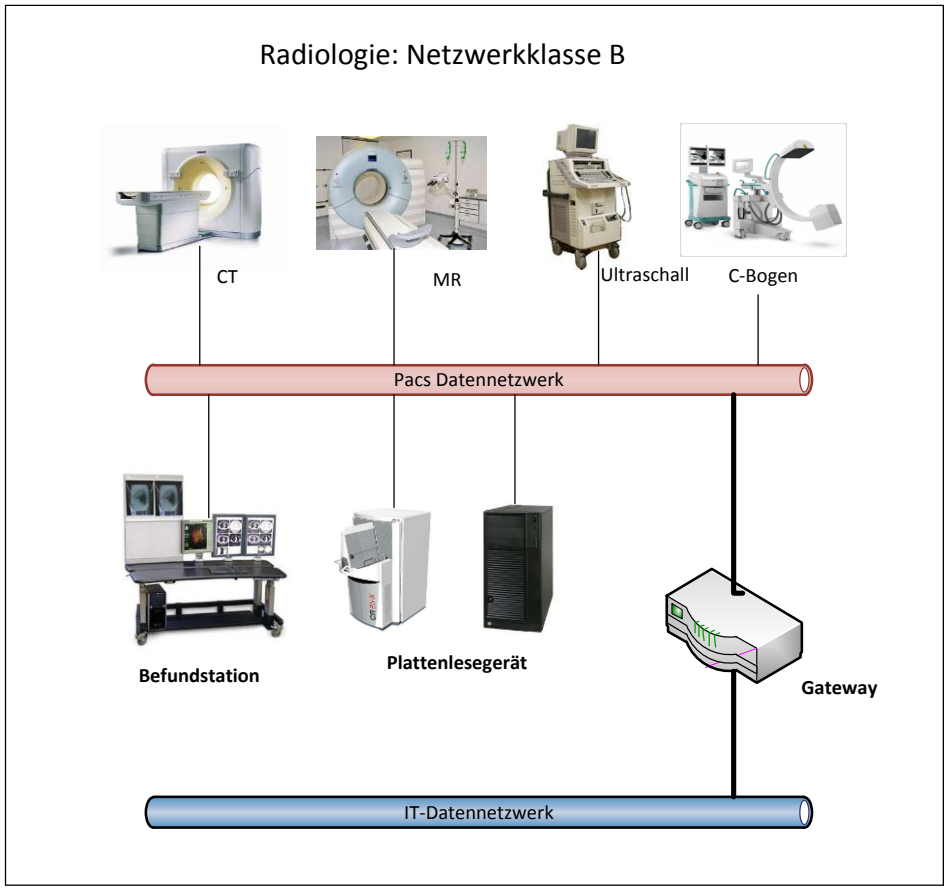

Abbildung 8: Netzwerkklasse B (DIN 60601-1 3rd)

3.8.3 Netzwerkklasse C

Netzwerke der Klasse C werden für alle **zeitkritischen Anwendungen** und Prozesse verwendet, welche im Fehlerfalle eine hohe PatientInnengefährdung darstellen können. Als Beispiel dient ein intensivmedizinisches Netzwerk, welches zum Monitoring der Vitalwerte von PatientInnen verwendet wird. Die Norm erfordert nicht nur die physische oder logische Trennung des Netzwerkes, sondern auch die höchste Verfügbarkeit des Netzwerkes in Bezug auf Störungen und geplanten Wartungsabschaltungen.

Eine Variante zu dedizierten Netzwerkkomponenten bietet die Betriebsform „shared network“, bei dem die Trennung der Netze auf gemeinsam genutzten Netzwerkkomponenten durch Einführung sogenannter VLAN-(Virtuell LAN-)Technik durch logische Trennung der OSI-Schichten 2 und 3 erfolgt.

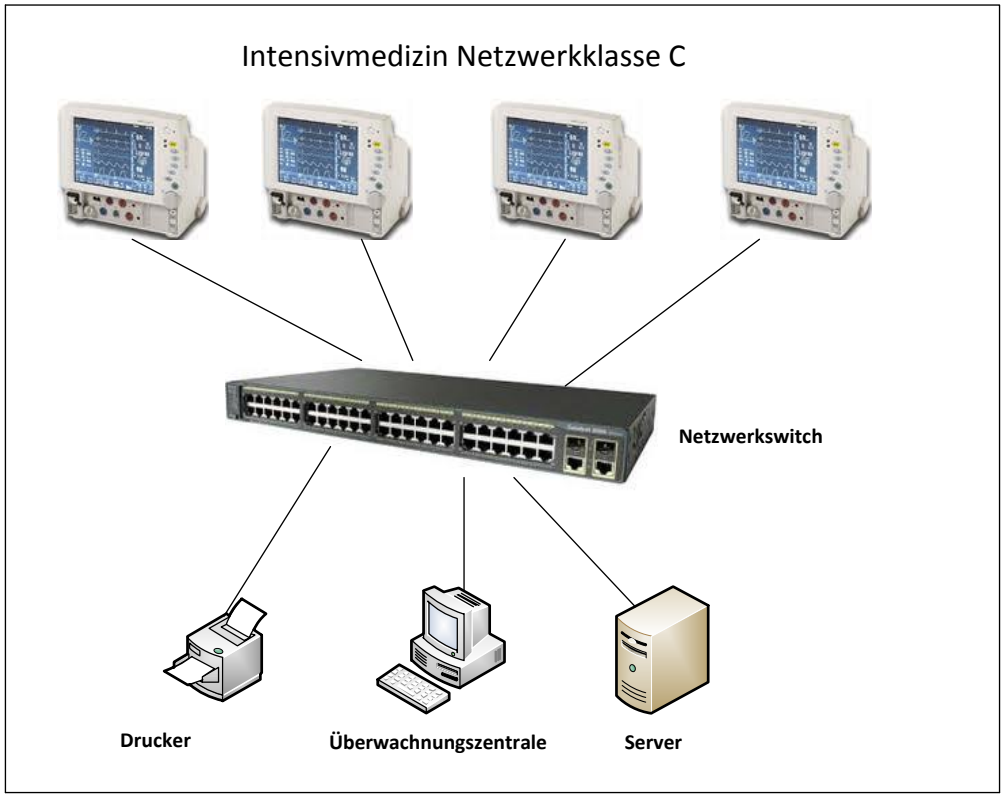

Abbildung 9: Netzwerkklasse C (DIN 60601-1 3rd)

4 IST-Analyse

Die IST-Analyse wurde am Beispiel der TILAK - Tiroler Landeskrankenanstalten GmbH durchgeführt. Die TILAK unternimmt unterschiedliche Anstrengungen, um Gefährdungen, welche sich laut Kapitel 3 im IT-Datennetzwerk der TILAK ergeben, zu begegnen.

Für IT/MT-Standardgeräte sind diese Schutzmaßnahmen am Stand der Technik, diese Geräte sind:

- mit einer aktuellen Windows-Version ausgestattet,
- enthalten die aktuellen Malware-Schutzprogramme
- in TILAK-weite Update-Mechanismen eingebunden
- in der Microsoft AD-Struktur der TILAK eingebunden
- von der IT-Abteilung der TILAK betreut.

Neben den Standardgeräten existieren im Netzwerk der TILAK allerdings auch Medizintechnikgeräte und Haustechnikgeräte, auf die obige Maßnahmen nicht bzw. nicht vollständig umgesetzt werden können („Nicht-Standardgeräte“).

Früher waren Medizintechnikgeräte und Medizintechniksysteme Insellösungen ohne Schnittstellen zu anderen Geräten und meist auch ohne Netzwerkanbindung. Wie eine durchgeführte IST-Erhebung bestätigt, bestehen solche Systeme gegenwärtig oft aus einem Geräteverbund mit unterschiedlichen Betriebssystemen und der Notwendigkeit, mit anderen Systemen (z.B. Labor-Informationssystem LIS, Klinisches Informationssystem KIS, …) über das Netzwerk zu kommunizieren. Dieser Trend wird sich zukünftig weiter verstärken.

Oft werden medizintechnische Systeme vom Hersteller mit einer gewissen Softwareversion ausgeliefert, die vom Kunden nicht an die bestehenden Sicherheitsstandards bezüglich Domäneneinbindung, Updatezyklus und Schutz gegen schädliche Software, angepasst werden darf, da sonst die Zertifizierungen oder Garantien verloren gehen.

Die Erfahrungen der letzten Jahre zeigen, dass aktuelle Updates von Betriebssystemen und Virenschutzkomponenten unerlässlich sind, um sich vor der Ausnutzung von Sicherheitslücken durch Schadsoftware zu schützen. Hinzu kommt, dass es innerhalb des Netzwerkes der TILAK keine abgegrenzten Netzwerkbereiche für diese ungeschützten Systeme gibt und keine Detaildokumentation über den Konfigurationsstand und das Kommunikationsverhalten existiert.

Das Schutzniveau der an das Netzwerk angeschlossenen „Nicht-Standardgeräte“ ist in der Folge überwiegend als gering einzustufen.

Medizintechnikgeräte unterschiedlichster Ausprägung werden derzeit im LAN der TILAK betrieben. Bisher war es nicht möglich, Geräte, die nicht dem hohen Schutzniveau der TILAK- Standard-Arbeitsplätze entsprechen, gegenüber Angriffen aus dem Netzwerk oder vor Infektionen durch Schadsoftware über das Netzwerk effizient abzusichern.

Fast alle der in Kapitel 4.1 angeführten Gerätegruppen benötigen eine Netzwerkverbindung ins TILAK-IT-Datennetz mit folgenden Begründungen:

- Datenaustausch mit anderen Rechnern (derzeit Laufwerksfreigabe)
- Datenaustausch mit weiteren Informationssystemen
- Fernwartung durch Hersteller und Wartungsfirmen

4.1 **Medizintechnische Gerätekategorien**

Im Zuge der IST-Erhebung und der Suche nach passenden Klassifikation der medizintechnischen Anlagen und Geräte zur Dokumentation der IST-Situation werden die eingesetzten Geräte nach einem Emtec-Code eingeteilt. Der Verein Emtec ist ein Netzwerk von Praktikern der Krankenhausplanung, von Krankenhausmanagern, Ärzten, Pflegekräften, Ingenieuren und Medizintechnikern.

Ziel des Vereins ist, aus den Erfahrungen bei Einsatz, Wartung und Instandhaltung medizintechnischer Geräte, sowie der Analyse von Ausfallursachen und Sicherheitshinweisen, Grundlagenwissen aufzubereiten und als Entscheidungshilfen zu publizieren bzw. als herstellerneutrales Fachwissen zu vermitteln. Folgende Tabelle ist ein Auszug aus dem Emtec-Gesamtkatalog:

Quelle: (Emtec e.v., 2011)

Medizintechnische Geräte	**Bezeichnung**	**Emtec-Code**
Vitalfunktion/Intensivmedizin	Beatmungsgeräte	WAA
	Inhalations-Narkosegeräte	WAB
	Beatmung und Narkose, Zusatzgeräte	WAC
	Inkubatoren und Wärmegeräte	WAG
	Notfallausrüstung	WAH
	Herz-Lungen-Systeme	WAJ
	Druckkammer	WAK
	Kreislaufbeeinflussungsgeräte	WAL
Stoffaustausch	Dialyse- und Blutfiltrationsgeräte	WBA
	Dialyse-Hilfsgeräte	WBC
	Infusionsapparate	WBD
	Absauggeräte	WBE
	Blutzufuhr-/ -entnahme/ -aufarbeitungsgeräte	WBG
	Bluttemperierungsgeräte	WBH
Funktionsdiagnostik	Neurologie-Messgeräte	WCA
	Elektrokardiographen	WCB
	Blutdruckmessgeräte	WCC
	Gefäßdiagnostik-Messgeräte	WCD

Medizintechnische Geräte	Bezeichnung	Emtec-Code
	Temperaturmessgeräte	WCE
	Ergometer	WCF
	Lungenfunktions-Messgeräte	WCH
	Reizstrom-Diagnosegeräte	WCJ
	Haut-/Gewebe-Diagnostikgeräte	WCK
	Urologie-Messgeräte	WCL
	Stethoskope	WCM
	Knochenmineraldichte-Messgeräte	WCN
	Tachymetrie-Messgeräte	WCO
	Vitalitätsprüfgeräte	WCP
	Funktionsdiagnostik-Aufzeichnungsgeräte	WCQ
	Enterologie-Spezialgeräte	WCR
	Kombinationsgeräte, Funktionsdiagnostik	WCS
PatientInnenüberwachungs-geräte	PatientInnenüberwachungsgeräte	WDA
	Einzelparametermessung, OP/Intensiv	WDB
	Temperaturmonitore	WDC
	Beatmungs- und Narkose-Monitore	WDD
	Neurologie-Monitore	WDE
	Kombinationsmonitore / -module	WDF
	Überwachungseinheiten, Ergänzungen	WDJ
	Telemetrie-Anlagen	WDK
	Perinatale Überwachung	WDL
Therapiegeräte	Kardiologie-Notfallgeräte	WEA
	Elektro-Therapiegeräte	WEB
	Wärmetherapiegeräte/ Diathermiegeräte	WEC
	Bestrahlungsgeräte (nicht radiologisch)	WED
	Physiotherapiegeräte	WEE
	Stimulationsgeräte Nerven/ Muskeln, Therapie	WEF
	Sauerstoff-Therapiegeräte	WEG
	Kältetherapiegeräte	WEH
	Rehabilitationshilfen	WEK
Bildgebende Systeme	Röntgen-Aufnahmegeräte	WFA
	Durchleuchtungsgeräte	WFB
	Systemkomponenten, Röntgen	WFC
	Röntgen-Generatoren	WFD
	Röntgenspezialgeräte	WFE
	Röntgenfilmentwicklungsmaschinen	WFF
	Computertomographen	WFG
	Ultraschall-Diagnosegeräte	WFH
	Thermographie-Geräte	WFJ
	Nuklear-Diagnosegeräte	WFK
	Kernspintomographen	WFL
	Optische Tomographen	WFM
	Bildaufzeichnungs- und Dokumentationseinr.	WFP
	Bildbetrachtungseinrichtungen	WFR
Strahlentherapie	Afterloading-Geräte	WGA
	Telegamma-Geräte	WGB
	Strahlentherapie-Beschleuniger	WGD
	Bestrahlungseinrichtungen f. Probenmaterial	WGF
Medizinische Physik/ Strahlenschutz	Strahlungs-Messgeräte	WHA
	Messphantome (Medizinische Physik)	WHB
	Messgeräte (allgemein) Medizinische Physik	WHC
Chirurgie/Endoskopie	HF-, Wärme-, Kälte-Chirurgiegeräte	WJA
	Laser-Chirurgiegeräte	WJB
	Ultraschall-Chirurgiegeräte	WJC
	Chirurgiegerät, energetisch	WJD

Medizintechnische Geräte	Bezeichnung	Emtec-Code
Laborgeräte	Labor-Zentrifugen	WKA
	Apothekengeräte	WKF
	Analysatoren, einfach	WKG
	Chromatographiegeräte	WKH
	Analysatoren, Hämatologie	WKI
	Analysatoren, Labor	WKJ
	Mikroskope	WKK
	Photometer	WKL
	Analysatoren, Klinische Chemie	WKM
	Refraktometer/ Dilatometer	WKN
	Messgeräte, Einzelmessung, Labor	WKP
	Immunologisch-Infektionsserologische Laboreinrichtung	WKQ
	Molekularbiologische Laboreinrichtung	WKR
	Mikrobiologisch-Serologische Laboreinrichtung	WKS
	Spektroskopiegeräte	WKT
	Diffraktometriegeräte	WKU
	Analysatoren, Nuklear-Labor	WKV
	Pathologie- und Histologie-Laborgeräte	WKW
	Pathologiegeräte	WKZ
Fachärztliches Gerät	Ophthalmologische Geräte	WNA
	HNO-Geräte	WNB
	Dentalmedizinische Geräte	WNC
	Dentaltechnische Geräte	WND
Desinfektion, Sterilisation	Desinfektionsgeräte	WOA
	Sterilisationsgeräte	WOB
	Desinfektion / Sterilisation-Zusatzgeräte	WOC

Tabelle 2: Geräteklassen nach Emtec

4.2 Vorhandene Schutzmaßnahmen

Die TILAK ist Mitglied des österreichischen akademischen Wissenschaftsnetzes (ACO-NET[1]), welches den Zugang zum internationalen Wissenschaftsnetz GEANT[2] und zum Internet bietet.

In den Tiroler Landeskrankenanstalten (TILAK) sind derzeit folgende Schutzmaßnahmen im Bereich Internetanbindung, Serversystemen und bei den Clients im Einsatz:

System	Schutzsystem	Hersteller
Internetanbindung	Firewall-System	Barracuda-Phion-Netfence
	Mailwareschutz Mail	McAfee E-Mail-Security-Appliance
	Mailwareschutz HTTP	McAfee Web-Security-Appliance
	VPN IP-Sec-Zugang	Barracuda-Phion

[1] Austrian Academic Computer Network
[2] GÉANT ist das pan-europäische Internet-Verbindungsnetzwerk der europäischen Forschung

System	Schutzsystem	Hersteller
Windows-Server-Systeme	Mailwareschutz	Microsoft Forefront
	Updateservice	Microsoft WSUS
Unix-Server-Systeme	keine	keine
Linux-Server-Systeme	keine	keine
Windows-Clients	Mailwareschutz	McAfee Endpoint-Protection
	Updateservice	Microsoft WSUS[3]
Linux-Clients	keine	keine
Mac OS	keine	keine

Tabelle 3: TILAK-Schutzsysteme

4.3 Vorhandene Client-Betriebssysteme

In den Tiroler Landeskrankenanstalten (TILAK) sind derzeit folgende Client-Betriebssystemarten im Einsatz. In nachfolgender Tabelle werden beispielhaft die verschiedensten Betriebssysteme zu Gruppen zusammengefasst:

Betriebssystemarten	Bezeichnung
Microsoft	Windows 2000, XP, Vista; Windows 7
Linux	Debian, Red Hat, SuSe
Apple	Mac OS-Familie
Unix System 5	AIX, HP-UX, Solaris
PDA Smartphone-Betriebssysteme	Apple IOS, Android, Symbian, Win7
Eingebettete Betriebssysteme	CatOS, IOS, GNU, OSEK

Tabelle 4: Betriebssystemarten

[3] Windows Server Update Services (WSUS)

5 Lösungsansätze

Der Lösungsansatz wird am Beispiel der Tiroler Landeskrankenhäuser (TILAK) durchgeführt und diese Methode kann jederzeit auch auf andere Institutionen angewandt werden.

5.1 **Mapping: Gefährdung zur Schutzmaßnahme**

In nachstehender Tabelle werden die Gefährdungen laut Kapitel 2 mit den möglichen Schutzmaßnahmen von Kapitel 3 in einer Tabelle in Relation gebracht.

Gefährdung		Schutzmaßnahme											
			Firewall ohne IDS/IPS	IDS/IPS	Malwareschutz	E-Mail-Spam-SPY-Filter	URL-Filtering	Authentifizierung	Verschlüsselung	Aktueller Patchlevel	Netzwerkkategorisierung DIN 60601	Einführung ISO/IEC 27001	MPG, MPBV, Einführung DIN ISO/IEC 80001
	Höhere Gewalt	Feuer										X	
		Hochwasser										X	
		Erdbeben										X	
	Organisatorische Mängel	Notfallplanung										X	X
		Personalplanung										X	X
		Vertretungsregelung										X	X
		Schulung										X	X
		Wartungspatches										X	X
	Menschliches Fehlverhalten	Bedienungsfehler										X	X
		Unabsichtliche Datenlöschung										X	X
		Konfigurationsfehler										X	X
	Technisches Versagen	Hardwarefehler										X	X
		Softwarefehler		X						X		X	X
	Vorsätzliche Handlungen	Zugriffsverletzung	X	X				X			X	X	
		Malwarebefall		X	X	X	X			X	X	X	
		Denial of Service		X							X	X	
		Nachrichtenverzögerung		X							X	X	
		Nachrichtenverfälschung		X					X		X	X	
		Wiederholungsangriffe		X							X	X	

Tabelle 5: Mapping: Gefährdung - Schutzmaßnahme

In weiterer Folge werden die möglichen Gefährdungen in der Matrix beurteilt:

Höhere Gewalt

Als Schutzmaßnahme gegen diese Gefährdung ist die Einführung eines Informations-Sicherheitsmanagement-Systems nach IEC-Norm 27001 sinnvoll. In der Tilak wird an der Einführung eines Informationssicherheitssystems gearbeitet und es stellt eine sinnvolle Maßnahme zur Verhinderung der Gefährdung durch „Höhere Gewalt“ dar.
Quelle: (IEC 27001, 2008)

Organisatorische Mängel

Mit diesem Themenbereich befasst sich intensiv die neue Norm DIN EN-80001. Der Focus dieser Norm liegt im Bereich Risikomanagement von Netzwerken, an denen Medizinprodukte angeschlossen sind. Der Bereich Aufgaben und Definition der Verantwortlichkeiten wird in dieser Norm im Kapitel 3 „Rollen und Verantwortlichkeiten“ genau geregelt.
Quelle: (IEC 80001, 2010)

Menschliches Fehlverhalten

Bei dieser Gefährdung gilt der gleiche Lösungsansatz wie beim Themenbereich „Organisatorische Mängel“. Ein wesentlicher Bereich der DIN Norm EN-80001 beschäftigt sich im Kapitel 3 und 4 mit dem Bereich Risikomanagement zur Verhinderung von Gefährdungen im Bereich der Kategorie „Menschliches Versagen“.

Technisches Versagen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI Grundschutz, 2011) listet insgesamt 73 Gefährdungen zu diesem Themenkomplex auf. Als Schutzmaßnahme für diese Gefährdung ist eine Einführung eines Informations-Sicherheitsmanagement-Systems nach IEC-Norm 27001 und das Einhalten der Medizinprodukte-Betreiberverordnung sinnvoll.

Vorsätzliche Handlungen

Dieser Gefährdung kann durch die verschiedensten technischen Schutzmaßnahmen wie Malwareschutzsysteme, Firewall-Systeme und Intrusion-Prevention-Systeme entgegengewirkt werden. Eine detaillierte Analyse der möglich Einsatzmöglichkeiten und Konzepte wird in den nächsten Kapiteln beschrieben.

Zusammenfassend kann man die möglichen Gefährdungen durch folgende Schutzmaßnahmen abwenden.

Gefährdung	Mögliche Schutzmaßnahme
Höhere Gewalt	Einführung DIN ISO/IEC 27001
Organisatorische Mängel	Einführung DIN ISO/IEC 80001, MPG, MPBV
Menschliches Fehlverhalten	Einführung DIN ISO/IEC 80001, MPG, MPBV
Technisches Versagen	Einführung DIN ISO/IEC 27001, MPG, MPBV
Vorsätzliche Handlungen	Einführung Techn. Schutzmaßnahmen

Tabelle 6: Gegenüberstellung Gefährdung zu Schutzmaßnahme

Eine Einführung bzw. die Umsetzung der Normen der Serien

- DIN ISO/IEC 60601 „Medizinische elektrische Geräte, allg. Festlegung Sicherheit“
- DIN ISO/IEC 27001 „IT-Sicherheit Informationssicherheits-Management-System“
- DIN ISO/IEC 80001 „ Risikomanagement von Netzwerken mit Medizinprodukten“

kann die möglichen Gefährdungen laut Bundesamt für Sicherheit in der Informationstechnik wesentlich verringern.

Die Gefährdung durch vorsätzliche Handlungen kann durch den Einsatz von technischen Schutzsystemen verringert werden und daher wird dieser Themenbereich in dieser Diplomarbeit genauer betrachtet.

5.2 Mapping: Techn. Schutzmaßnahmen mit vorhandenen techn. Schutzmaßnahmen

In nachstehender Tabelle werden die technischen Schutzmaßnahmen laut Kapitel 3 mit den vorhandenen technischen Schutzmaßnahmen von Kapitel 4 in einer Tabelle in Relation gebracht.

		Firewall ohne IDS/IPS	IDS/IPS	Malwareschutz	E-Mail-Spam-Spy-Filter	URL-Filtering	Authentifizierung	Verschlüsselung	Aktueller Patchlevel
Vorsätzliche Handlungen	Zugriffsverletzung	X	X				X		
	Malwarebefall		X	X	X	X			X
	Denial of Service		X						
	Nachrichtenverzögerung		X						
	Nachrichtenverfälschung		X					X	
	Wiederholungsangriffe		X						

Tabelle 7: Mapping Techn. Schutzmaßnahmen / Gefährdungen

- Schutzmaßnahme erfüllt
- Schutzmaßnahme teilweise erfüllt
- Schutzmaßnahme nicht erfüllt

Firewall ohne IDS-/ IPS-Funktion

Das vorhandene Firewall-System dient zur Absicherung des redundanten Internetanschlusses und der DMZ-Zonen. Derzeit sind keine Subnetz-Firewall-Systeme zur Absicherung der medizintechnischen Geräte im Einsatz und daher ist diese Schutzmaßnahme nur zum Teil erfüllt.

IDS-/ IPS-System

Derzeit sind bei den Tiroler Landeskrankenanstalten keine IDS-/ IPS-Systeme im Einsatz.

Malwareschutz

Derzeit wird das Produkt „McAfee Endpoint-Protection“ für Windows-Clients in der Tilak verwendet. Für die restlichen Betriebssysteme der Tabelle 4 sind keine Malware-Schutzprogramme im Einsatz, da für diese Betriebssysteme der Schadsoftwarebefall wesentlich geringer als bei Windows-Systemen einzustufen ist. Meistens werden medizintechnische Geräte mit einem gewissen Softwaresetup ausgeliefert, bei denen keine Malware-Schutzprogramme installiert werden dürfen, da Zertifizierungen und Garantieansprüche seitens der Hersteller verloren gehen würden. Weiters ist zu beachten, dass die Verantwortung für einen funktionierenden Malwareschutz auf den medizintechnischen Geräten in der Tilak in der Fachabteilung Medizin- und Labortechnik liegt und aufgrund dieses organisatorischen Hintergrundes wird diese Schutzmaßnahme nur zum Teil erfüllt.

E-Mail-Spam und Spy-Filterung

Für diese Gefährdung wird netzbasierend das Produkt „McAfee Web-Security-Appliance“ und zusätzlich beim Mailserversystem Microsoft Exchange das Schutzsystem „Microsoft Forefront for Exchange“ eingesetzt. Aus diesen Gründen kann diese Schutzmaßnahme als erfüllt eingestuft werden.

Authentifizierung

Im Bereich des Netzwerkes kann die generelle Methode für die Authentifizierung und Autorisierung in IEEE 802-Netzen nach dem Standard IEEE 802.1X erfolgen. Derzeit wird in der Tilak diese Methode bei den mobilen Wireless-Geräten eingesetzt, Diese Methode soll auch bei den physischen Ports eingeführt werden. Aus diesen Gründen kann diese Schutzmaßnahme als teilweise erfüllt eingestuft werden.

Verschlüsselung

Derzeit sind bei den Tiroler Landeskrankenanstalten keine Verschlüsselungssysteme im Bereich der Datenübertragung für nicht mobile Endgeräte im Einsatz.

Aktueller Patchlevel

An den Standard-Windows-Clients, welche in der Microsoft-Domäne integriert sind, werden die aktuellen Windows-Patches mittels Windows-Update-Services durchgeführt. Medizintechnische Geräte sind größtenteils nicht Mitglied der Domäne und dürfen daher oft nicht mit dem notwendigen aktuellen Patchlevel versehen werden, da Zertifizierungen und Garantieansprüche seitens der Hersteller verloren gehen würden. Weiters ist zu beachten, dass die Verantwortung für ein funktionierendes Update-Service auf den medizintechnischen Geräten in der Tilak in der Fachabteilung Medizin- und Labortechnik liegt. Technisch und organisatorisch ist daher diese Schutzmaßnahme nur zum Teil erfüllt.

5.3 Client-Risikoklassen in Bezug auf das Betriebssystem

Folgende Tabelle klassifiziert Medizintechnikgeräte hinsichtlich ihres Gefährdungspotenzials durch das eingesetzte Betriebssystem.

Klasse	Bezeichnung	Beschreibung	Klassifizierung	Begründung
I	Proprietäre Systeme	Systeme mit proprietären Betriebssystemen, z.B. Wandler, Steuergeräte, Drucker, embedded Systeme, o.ä.	unkritisch	Geräte dieser Klasse stellen üblicherweise kein attraktives Ziel für Schadsoftware dar. Zusätzlich fehlt solchen Geräten oft auch die Fähigkeit zur Ausführung von Schadcodes.
II	Nicht-Windows -Systeme	Systeme mit Unix-Derivaten, Linux-Derivaten, MacOS oder anderen nicht MS Windows-Betriebssystemen	wenig kritisch	Nicht-Windows-Systeme sind durch ihre im Vergleich zu Windows-Systemen geringe Verbreitung nicht das bevorzugte Ziel von Schadsoftware und derzeit daher noch „wenig kritisch“.
III	Geräte mit definiertem Sicherheitsstandard	Darunter fallen Geräte, die einen definierten Sicherheitsstandard erfüllen, wie zum Beispiel: • TILAK-Standard-Client-PCs in der Domäne • Managed TILAK-IT-Clients	unkritisch	Geräte mit definiertem Sicherheits-Standard innerhalb der TILAK werden als ausreichend abgesichert gegen Schadsoftware angesehen.
IV	Systeme mit ungewarteten Microsoft Windows Betriebssystemen	Betriebssystem ist ungewartet. Die Wartung der Applikation erfolgt entweder durch Lieferanten oder überhaupt nicht.	kritisch	Ungewartete Windows-Systeme stellen durch die hohe Verbreitung des Betriebssystems ein beliebtes Angriffsziel dar und sind daher kritischer einzustufen als alle anderen Klassen.

Tabelle 8: Client-Risikoklassen

5.4 Lösungsansatz technische Schutzmaßnahmen

Aus obigen Betrachtungen lassen sich folgende Schlussfolgerungen bezüglich der einsetzbaren technischen Schutzmaßnahmen in Kontext mit den Client-Risikoklassen machen:

- Für Geräte der Risikoklassen I und II besteht kein akuter Handlungsbedarf.
- Für Windows-Geräte ist grundsätzlich danach zu trachten, ausschließlich Systeme einzusetzen, die die aktuellen Sicherheits-Standards erfüllen (Risikoklasse III). Diese Variante weist das höchste Sicherheitsniveau auf und vermeidet Zusatzkosten für den Einsatz externer Schutzmaßnahmen.
- Für Medizintechnikgeräte der Risikoklasse IV, an denen keine Änderungen vorgenommen werden dürfen, kommen Host-basierende Maßnahmen nicht in Frage und es müssen daher netzwerkbasierende Schutzmaßnahmen eingesetzt werden.
- Firewalls sind für das Bedrohungsszenario nicht als optimale Schutzmechanismen einsetzbar und nur bedingt eine geeignete Lösung zum Schutz der medizintechnischen Geräte.
- **Network Intrusion-Detection/ Prevention-Systeme (NIPS) sind aufgrund der Analysen in Kapitel 5.2 die optimale netzwerkbasierende Lösung für den Schutz medizintechnischer Geräte.**

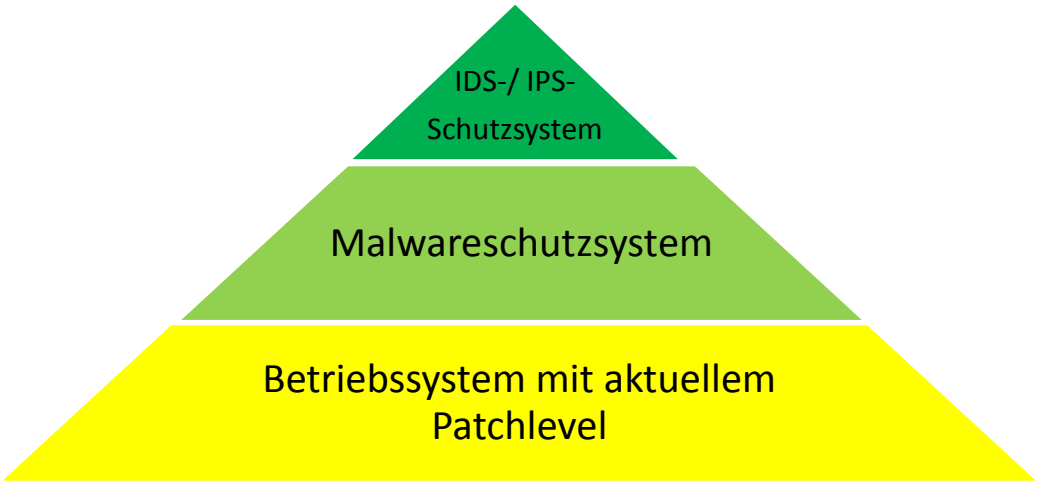

Abbildung 10: Schutzsystem-Pyramide

5.5 Lösungsansatz "Individueller Schutz einzelner Geräte"

In dieser Variante würde zwischen Netzwerkport am Etagenswitch und einem medizintechnischen Gerät mit Anbindung an das LAN ein lokales IPS installiert werden. Einsatzbereiche wären z.B. Etagen, auf denen nur wenige Medizintechnikgeräte ohne besondere Performance-Anforderungen geschützt werden müssen.

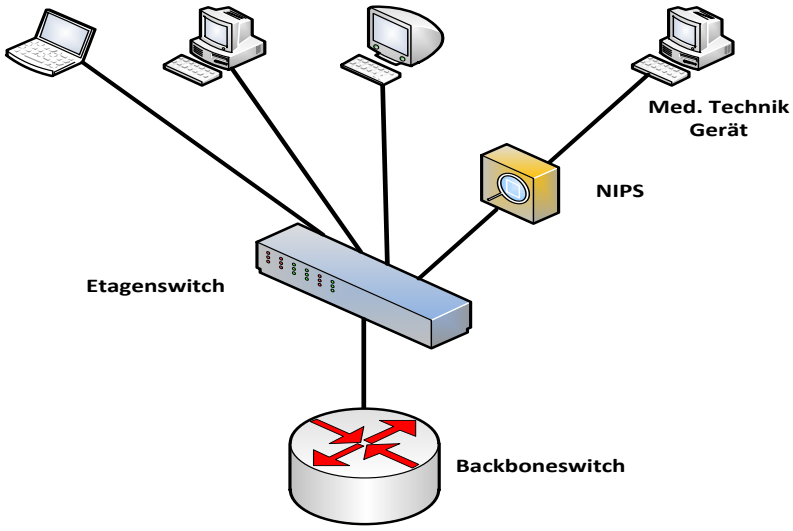

Abbildung 11: NIPS-Host-Lösungsansatz

Funktionelle Redundanz wäre möglich, falls das Endgerät über zwei Netzwerkschnittstellen verfügt und an unterschiedlichen Etagenswitches angebunden ist. In diesem Fall würde einfach ein „Mini-NIPS“ zwischen die Netzwerkanbindungen des Endgerätes und der Etagenswitches gesteckt werden.

Vorteile	Nachteile
Günstiger Einzelpreis durch niedrigere Performance-Anforderungen.	Diese Variante könnte eine hohe Anzahl an NIPS (inkl. Installationsaufwand usw.) nach sich ziehen, die auch verwaltet werden müssen.
Hohe Schutzwirkung durch hohe Segmentierung.	Zentrales Management durch die hohe Anzahl an NIPS unbedingt erforderlich.
Hoch skalierbar (Verwendung unterschiedlich performanter NIPS).	Erhöhte Netzwerklast durch regelmäßige Updates aller NIPS.
Keinerlei Eingriff in Switch-Konfiguration notwendig.	

Tabelle 9: Vorteil-Nachteil hostbasierender Ansatz

5.6 Lösungsansatz Variante „Etagenbasierter Schutz“

In dieser Variante wird ein Network-Intrusion-Prevention-System (NIPS) am Etagen-Switch installiert, über den der Verkehr von mehreren lokalen medizintechnischen Geräten dieser Etage mittels VLANs realisiert wird.

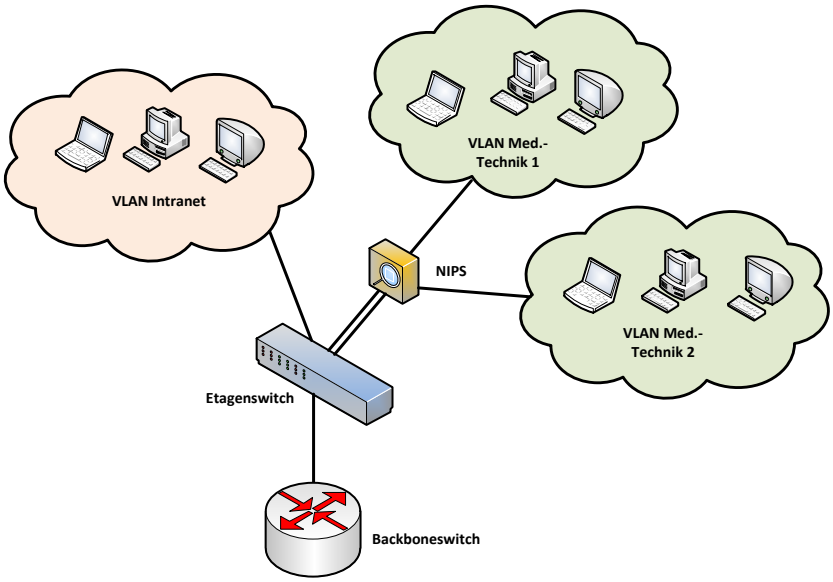

Abbildung 12: NIPS-Etagenlösungsansatz

Je nach Gegebenheiten könnten die medizintechnischen Geräte z.B. in VLANs auf Raum-, Hersteller- oder Gerätetypbasis getrennt werden. Notwendig sind bei diesem Ansatz zumindest ein NIPS pro Etage, sowie der Einsatz einer zentralen Management-Konsole zur Verwaltung aller NIPS. Einsatzbereiche sind z.B. Etagen, auf denen mehrere Medizintechnikgeräte geschützt werden müssen und eine logische Zusammenfassung dieser Geräte sinnvoll ist.

Vorteile	Nachteile
VLANs auf Etagen-Switches ausreichend (geringere Stückzahl als Lösungsansatz Variante „Etagenbasierter Schutz“)	Zentrales Management durch die hohe Anzahl an NIPS unbedingt erforderlich.
Hohe Schutzwirkung durch starke Segmentierung.	Eingriff in Konfiguration der Etagenswitches notwendig.
Hoch skalierbar, Verwendung unterschiedlich performanter NIPS.	Teilweiser Eingriff in die Verkabelung notwendig.

Tabelle 10: Vorteil-Nachteil etagenbasierender Ansatz

5.7 Lösungsansatz Variante „Backbone-basierender Schutz pro Standort“

In dieser Variante würde am Backbone-Switch jedes Hauses ein NIPS installiert werden, über das der Verkehr von mehreren medizintechnischen Geräten in verschiedenen Etagenverteilern mittels VLAN realisiert wird (was – im Prinzip - auch derzeit schon der Fall ist).

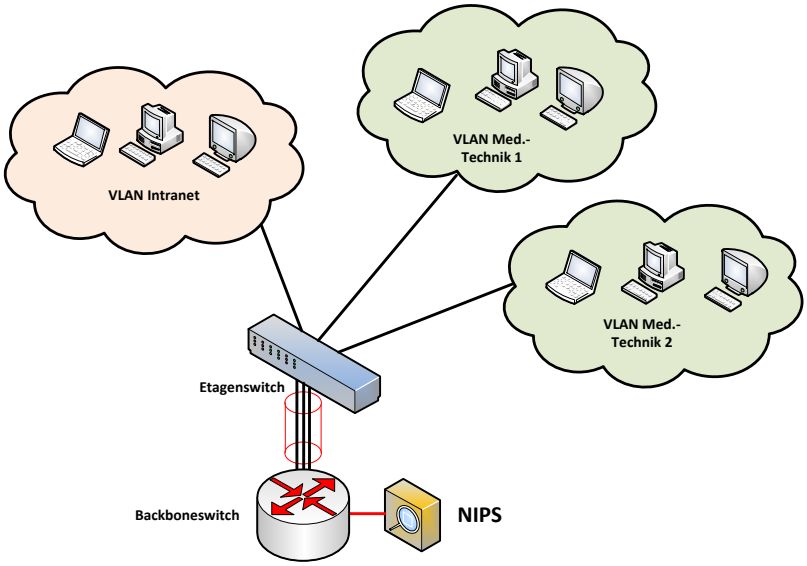

Abbildung 13: NIPS-Backbone-Lösungsansatz

In dieser Variante ist ein erhöhter Konfigurationsaufwand hinsichtlich Redundanz notwendig. Theoretisch können IPS auf den Backbone-Switches zum Einsatz kommen. Dabei ist allerdings zu bedenken, dass die Bandbreite der verfügbaren Geräte nicht an jene eines „Stand-Alone“-NIPS herankommt und, dass alle im LAN verwendeten NIPS von einer Management-Konsole aus verwaltet werden sollten.

Vorteile	Nachteile
Geringere Geräteanzahl als bei obigen Varianten.	Einheitliches zentrales Management durch die Anzahl an NIPS zumindest empfehlenswert.
Funktionelle Redundanz ist möglich.	Eingriff in Konfiguration der Etagenswitches und der Backbone-Switches notwendig.
Theoretisch ist IPS-Blades auf den Core-Switches einsetzbar.	Bandbreitenlimitierung durch Blade-Einsatz möglich.
VLANs müssen nicht über Zentrale geführt werden.	

Tabelle 11: Vorteil-Nachteil backbonebasierender Ansatz

6 Ergebnisse und Ausblick

Im abschließenden Kapitel werden die gewonnenen Ergebnisse zusammengefasst und eine Bewertung hinsichtlich der Umsetzbarkeit durchgeführt. Weiters wird ein Ausblick auf die weiteren möglichen Implementierungsschritte aufgezeigt.

6.1 Ergebnisse

Dieses Diplomarbeitsthema „Informationssicherheitskonzept für die Integration von medizintechnischen Geräten in ein IT-Datennetz“ beschäftigt mich schon einige Jahre in meiner Funktion als Verantwortlicher für den Bereich Informationstechnik bei den Tiroler Landeskrankenanstalten (TILAK). Durch diese Diplomarbeit konnten ich mich mit diesem sehr komplexen Themenbereich auseinandersetzten, insbesondere durch das Studium der Fachliteratur, den Besuch von Fachinformationsveranstaltungen und durch die Konsultation unserer Experten im Bereich Medizintechnik in unserem Haus.
Neben den allgemeinen Sicherheitszielen im IT-Datennetz, ist der Themenkomplex Informationssicherheit sehr gut vom Bundesamt für Sicherheit in der Informationstechnik (BSI Grundschutz, 2011) aufbereitet und bildet zusammen mit der einschlägigen Fachliteratur eine sehr gute Grundlage für diese Arbeit.
Die Integration von medizintechnischen Anlagen in ein IT-Datennetz obliegt einigen gesetzlichen Anforderungen und Normen. Der Betrieb dieser Anlagen obliegt einerseits der Medizinprodukte-Betreiberverordnung (MPBV) für die Krankenhausträger auf Basis des Medizinproduktegesetztes (MPG).
Weiters spielen Normen bei der Integration von medizintechnischen Geräten eine wesentliche Rolle. Neben der Norm DIN ISO/IEC 60601 „Medizinisch elektrische Geräte“ wird die physische Integration in das IT-Datennetz unter Berücksichtigung der elektrischen Schutzmaßnahmen gegen eine mögliche PatientInnengefährdung behandelt. In der neuen Norm DIN ISO/IEC 80001 werden die Themenbereiche Begrifflichkeiten, Aufgaben, Verantwortlichkeiten, Dokumentenkontrolle und der Bereich Risikomanagement beim Betrieb von medizintechnischen Anlagen geregelt. Die allgemeine Norm DIN ISO/IEC 27001 wurde entwickelt, um ein Modell für die Einführung, Umsetzung und Überwachung des Informationssicherheits-Managementsystems bereitzustellen. Sehr viele Themen- bzw. Aufgabenbereiche überschneiden sich in den verschiedenen Normen und gesetzlichen Anforderungen.

Aufgrund der Analyse der möglichen technischen Maßnahmen, um die potenziellen Gefährdungen für einen sicheren Betrieb zu ermöglichen, konnte festgestellt werden, dass einerseits das eingesetzte Betriebssystem, andererseits die Vorgaben der Gerätehersteller in Bezug auf mögliche einsetzbare Schutzmaßnahmen und die Verwendungsart der Geräte, eine wesentliche Rolle spielen. Die technische Anschaltung an das IT-Datennetzwerk wird durch die mögliche Gefährdung für den Patienten/ die Patientin geregelt.

Dies kann von einem völlig isolierten Betrieb (z.B. Chirurgie-Roboter) bis hin zur Integration (z.B. EKG-Gerät ohne Notfalleinsatz) in das IT-Netzwerk ohne zusätzliche Schutzmaßnahmen erfolgen.
Hostbasierende Schutzsysteme wie laufende Aktualisierung von Sicherheitspatches, Einsatz von Malwareschutzsystemen und hostbasierende IPS-Systeme können nur zum Teil eingesetzt werden, da die Herstellerzertifizierung verloren gehen würde und hostbasierende Schutzsysteme in der Regel nur für Windows-Betriebssysteme eingesetzt werden.
Eine weitere wesentliche Rolle liegt im Verantwortungsbereich der Betriebsführung von medizintechnischen Geräten. Geräte können seitens der IT-Abteilung nur als sicher eingestuft werden, wenn diese einem zentralen Sicherheitsmanagement unterliegen.
Ein effektiver Schutz dieser medizintechnischen Geräte kann ausschließlich über Sicherheitsmaßnahmen auf Netzwerkebene erfolgen. Zusätzlich erhöhen hostbasierende Schutzmaßnahmen auf den einzelnen Geräten den Geräteschutz.
Da Netzwerk-Intrusion-Prevention-Systeme im Vergleich zu Firewalls und Malwareschutzsystemen mit zusätzlichen Sicherheitsmechanismen ausgestattet sind, und mit weniger Personalaufwand für Implementierung und Wartung dieser Systeme zu rechnen ist, wird diese Technologie zum Schutz von medizintechnischen Geräten mit Anschluss an das IT-Datennetz empfohlen. Als bester Kompromiss zwischen Aufwand, Skalierbarkeit und Wartungsaufwand wird der Lösungsansatz „Backbone basierender Schutz pro Standort“ mit einem zentralen Management bevorzugt.
Die Fragestellung laut Kapitel 1.3 dieser Diplomarbeit „Können medizintechnische Geräte im Hinblick auf die Verarbeitung, Speicherung und Übertragung von Informationen, bezüglich Vertraulichkeit, Verfügbarkeit und Integrität vor negativen Beeinflussungen durch spezielle organisatorische und technische Maßnahmen geschützt werden?“ kann aus oben angeführten Erkenntnissen und Umsetzungsvorschlägen positiv beantwortet werden.

6.2 **Ausblick**

Diese Diplomarbeit bildet die Grundlage zur Einführung von medizintechnischen Schutzmaßnahmen in Bereich der Tiroler Landeskrankenanstalten. Nachdem schon sehr viele Geräte an das IT-Datennetz angeschaltet sind, ist eine genaue Erhebung der angeschalteten Geräte notwendig und eine Klassifizierung nach Emtec (Emtec e.v., 2011) und der jeweiligen Client-Risikoklassen laut Kapitel 4.3 durchzuführen. Weiters ist auch die Anschaltung an das IT-Datennetz nach der DIN-Norm IEC 60601 zu überprüfen und gegebenenfalls anzupassen.
Aufgrund dieser Erhebung kann mit der Konzeption und der Implementierungsplanung der netzbasierenden Intrusion-Detection/ Prevention-Systeme begonnen werden. Diese Planung soll in weiterer Folge für die Beschaffung der Geräte verwendet werden. Nach erfolgter Bietersuche, Implementierungskonzeptanalyse, Produktauswahl und Auftragsvergabe kann mit der Implementierung der Systeme begonnen werden.
Im ersten Schritt sollten alle medizintechnischen Geräte der Klasse IV (Windows-Systeme ohne aktuellen Patchlevel und ohne Malwareschutz) mit den netzbasierenden Intrusion-Detection-Systemen (NIPS) geschützt werden.

Ab diesem Zeitpunkt müssen alle neu zu integrierenden medizintechnischen Geräte mit diesem NIPS-Schutzsystem versehen und die restlichen bereits installierten Systeme im Zuge von Wartungstätigkeiten auch umgestellt werden. Die Umstellung auf die speziellen Medizintechnik-VLANs hat eine Änderung der IP-Adresse auf den Geräten zur Folge.

Mit dieser Vorgehensweise könnten innerhalb eines absehbaren Zeitraumes von ca. zwei Jahren alle medizintechnischen Geräte mit den geplanten Schutzsystemen versehen werden.

Ein weiteres Projekt ist die Einführung eines Informationssicherheits-Management-Systems für die Tiroler Landeskrankenanstalten. Eine spezielle Herausforderung ist die Einführung der ISO 27001 unter Berücksichtigung der restlichen gesetzlichen Rahmenbedingungen wie Medizinproduktegesetz und Medizinprodukte-Betreiberverordnung. Weiters sind für IT-Systeme in den Laboren und in der Blutbank noch zusätzliche Verordnungen wie GMP (good manufactoring practice), PIC/S und Annex 11 (Implementierungsleitfaden für GMP) zu beachten.

Ziele dieser Tätigkeiten sind: Ziele und Maßnahmen zu definieren, um den geforderten gesetzlichen Rahmenbedingungen zu entsprechen und die aktuellen Sicherheitsrichtlinien für eine kontrollierte Systemumgebung zu schaffen. Eine ISO 27001-Zertifizierung der IT-Infrastruktur wäre dann der Abschluss des Projektes.

Literaturverzeichnis

McAfee Threat-Report 4Q2010. (2011). Abgerufen am 04.06.2011 von http://www.mcafee.com/de/resources/reports/rp-quarterly-threat-q4-2010.pdf

Beierlein, T., & et al. (2004). *Mikroprozessortechnik.* Mittweida: Fachbuchverlag Leipzig.

Bless, R. (2005). *Sichere Netzwerkkommunikation.* Karlsruhe: Springer Verlag.

BSI Grundschutz. (2011). *IT- Grundschutz Kataloge*. Abgerufen am 05.05.2011 von https://www.bsi.bund.de/DE/Themen/weitereThemen/ITGrundschutzKataloge/itgrundschutzkataloge_node.html

Bumerl, S. (2010). *Cryptas Consulting*. Abgerufen am 05.06.2011 von Cryptas Consulting.

ConSecur GmbH. (2002). *Einführung von Intrusion-Detection-Systemen.* Meppen.

Deal , R. (2005). *Cisco Router Firewall Security.* Indianapolis: Cisco Press.

Eckert, C. (2009). *IT-Sicherheit 6. Auflage.* München: Oldenburg Wissenschaftsverlag.

Emtec e.v. (2011). *Klassifizierung*. Abgerufen am 10.06.2011 von http://www.emtec.de

Frohberg, W., & et al. (2008). *Nachrichtentechnik.* Leipzig: Carl Hanser Verlag.

Gärtner, A. (2008). *Elektrische Sicherheit in der Medizintechnik.* Köln: TÜV Media.

Gärtner, A. (2010). *Medizinische Netzwerke und Software als Medizinprodukt, Band 5.* Köln: TÜV Media.

Herbert, K. (2006). *Viren, Würmer und Trojaner.* Tübingen: Klöpfer & Meyer.

IEC 27001. (2008). *DIN EN 27001-1 ISMS Informations-Sicherheits-Management-System.* IEC.

IEC 60601. (2008). *DIN EN 60601-1-6 Medizinische elektrische Geräte.* IEC.

IEC 80001. (2010). *DIN EN 80001-1 Risiko-Management Med. Netzwerke.* IEC.

Kaspersky, E. (2008). *Malware.* München: Carl Hanser Verlag.

Kraft, P., & et al. (2010). *Network Hacking.* Poing: Franzis Verlag.

Lipski, M. (2009). *Social Engineering.* Hamburg: Diploma Verlag.

Microsoft. (2011). *Sharepointcommunity*. Abgerufen am 20. 05 2010 von Sharepoint-community: http://live.sharepointcommunity.de/wiki/Downloads/SecureCcolaborationDt.pdf

Pohlmann, N., & et al. (2006). *Der IT-Sicherheitsleitfaden 2. Auflage.* Heidelberg: Redline GMBH.

Russel, J. (2004). *Gefahren aus dem Internet.* Norderstedt: Verlag für akademische Texte.

Schneider, U., & et al. (2007). *Taschenbuch der Informatik 6. Auflage.* Leipzig: Carl Hanser Verlag.

Siemers, C., & al., e. (2008). *Digitaltechnik 2. Auflage.* Nordhausen: Fachbuchverlag Leipzig.

Stein, E. (2008). *Rechnernetze und Internet 3. Auflage.* Jena: Carl Hanser Verlag.

Wikipedia. (2011). *Wiki Private IP-Adresse*. Abgerufen am 15.05.2011 von http://de.wikipedia.org/wiki/Private_IP-Adresse

Eidesstattliche Erklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.

Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Thaur, am 10. Juli 2011

Unterschrift

Ing. Romed Giner